VK2

VK2-2MPCCPL

VK2-2MPCCW

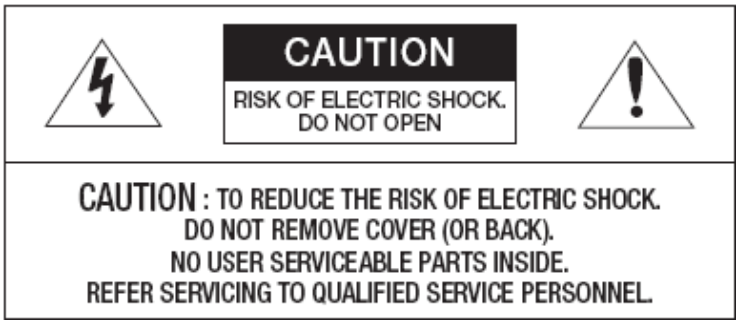
User manual

WARNING

TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS PROCUCT TO RAIN OR MOISTURE. DO NOT INSERT ANY METALLIC OBJECT THROUGH THE VENTILATION GRILLS OR OTHER OPENNINGS ON THE EQUIPMENT.

Apparatus shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the apparatus.

CAUTION



EXPLANATION OF GRAPHICAL SYMBOLS

The lightning flash with arrowhead symbol, within an equilateral triangle, is intended to alert the user to the presence of un-insulated "dangerous voltage" within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock.

The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

CAUTION: CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

CE 0678

TO COMPLY WITH RF EXPOSURE COMPLIANCE REQUIREMENTS, THE ANTENNA USED FOR THIS TRANSMITTER MUST BE INSTALLED TO PROVIDE A SEPARATION DISTANCE OF AT LEAST 20cm (7.9in) FROM ALL PERSONS AND MUST NOT BE CO-LOCATED OR OPERATING IN CONJUNCTION WITH ANY OTHER ANTENNA OR TRANSMITTER.

HEREBY, VISTA DECLARES THAT THIS PRODUCT IS IN COMPLIANCE WITH THE ESSENTIAL REQUIREMENTS AND OTHER RELEVANT PROVISIONS OF DIRECTIVE 1999/5/EC.

A COPY OF THE ORIGINAL DECLARATION OF CONFORMITY MAY BE OBTAINED FROM NORBAIN SD LTD (VISTA) 210 WHARFEDALE ROAD, IQ WINNERSH, WOKINGHAM RG41 5TP ENGLAND

THIS DIGITAL EQUIPMENT FULFILLS THE REQUIREMENTS FOR RF EMISSION ACCORDING TO THE CLASS B LIMIT OF EN 55022.

THIS PRODUCT FULFILLS THE REQUIREMENTS FOR IMMUNITY ACCORDING TO EN 55024 AND EN 50130-4 OFFICE AND COMMERCIAL ENVIRONMENTS.

CAUTION

RISK OF EXPLOSION IF THEBATTERY IS REPLACED WITH AN INCORRECT TYPE.

DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

IMPORTANT SAFETY INSTRUCTIONS

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.

13. Unplug this apparatus during lightning storms or when unused for long periods of time.
14. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
15. ***CAUTION – THESE SERVICING INSTRUCTIONS ARE FOR USE BY QUALIFIED SERVICE PERSONNEL ONLY. TO REDUCE THE RISK OF ELECTRIC SHOCK DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE OPERATING INSTRUCTIONS UNLESS YOU QRE QUALIFIED TO DO SO.***
16. ***Use satisfy clause 2.5 of IEC60950-1/UL60950-1 or Certified/Listed Class 2 power source only.***

ITE is to be connected only to PoE networks without routing to the outside plant.

1. DESCRIPTION 8

1.1 Components 8

1.2 Key Features 8

1.3 Overview 10

2. INSTALLATION 11

2.1 Connection 11

2.2 Network Connection and IP assignment 13

3. OPERATION 14

3.2. Access from the internet 15

3.3 Setting the admin password over a secure connection 15

3.4 Live View Page 16

3.5.1 Basic Configuration 18

3.5.2 Video & Image 26

3.5.3 Audio 31

3.5.4 Event 32

3.5.5 System 48

3.5.6 About 68

3.6 Playback 68

3.7 Help 70

3.8 Resetting to the factory default settings 71

4. APPENDIX 72

4.1 Troubleshooting 72

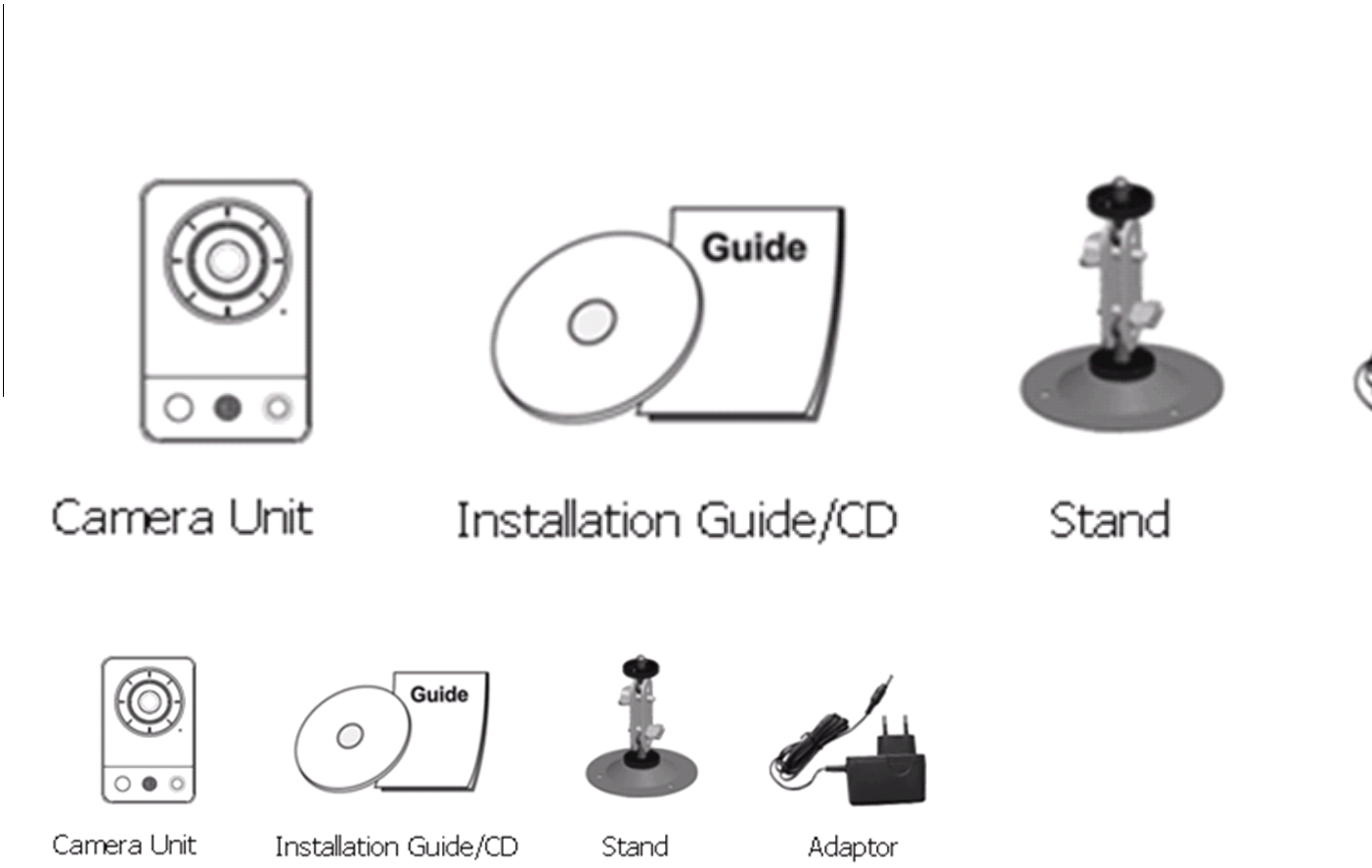
4.2 Product Specification 73

4.3 Preventive Maintenance 74

1. DESCRIPTION

This manual applies to the VK2-2MPCCW and VK2-2MPCCPL network camera.

Model main features



NOTE: Check your package to make sure that you received the complete system, including all components shown above.

1.2 Key Features

- **2 Mega pixel video quality**
  The Network Camera offers the highly efficient H.264 video compression, which drastically reduces bandwidth and storage requirements without compromising image quality. Motion JPEG is also supported for increased flexibility.

- **Dual or triple streams**
  The Network Camera can deliver dual or triple video streams simultaneously at full frame rate in all resolutions up to 2M(1600 x 1200) using Motion JPEG and H.264 (or MPEG-4). This means

that several video streams can be configured with different compression formats, resolutions and frame rates for different needs.

- **Image setting adjustment**
  The Network Camera also enables users to adjust image settings such as contrast, brightness and saturation to improve images before encoding takes place.

- **Intelligent video capabilities**
  The Network Camera includes intelligent capabilities such as enhanced video motion detection. The network camera's external inputs and outputs can be connected to devices such as sensors and relays, enabling the system to react to alarms and activate lights or open/close doors.

- **Micro-SD Recording support**
  The Network Camera also supports a micro-SD memory slot for local recording with removable storage.

- **Improved Security**
  The Network Camera logs all user access, and lists currently connected users. Also, its full frame rate video can be provided over HTTPS.

- **PIR Sensor (VK2-2MPCCPL)**
  Complementing the video motion detection capability of the cameras, the full-featured VK2-2MPCCPL additionally integrates a PIR Sensor for detecting movements - even in the dark.

- **Illumination (VK2-2MPCCPL)**
  VK2-2MPCCPL offers a white LED for illuminating the scene automatically at an event or when requested by the user.

- **Microphone and speaker (VK2-2MPCCPL)**
  VK2-2MPCCPL provides two-way audio support with integrated microphone and speaker, allowing remote listening in on an area as well as communication with persons entering the scene. An event can trigger the sound of an audio clip, stored in the camera, to be emitted through the speaker.

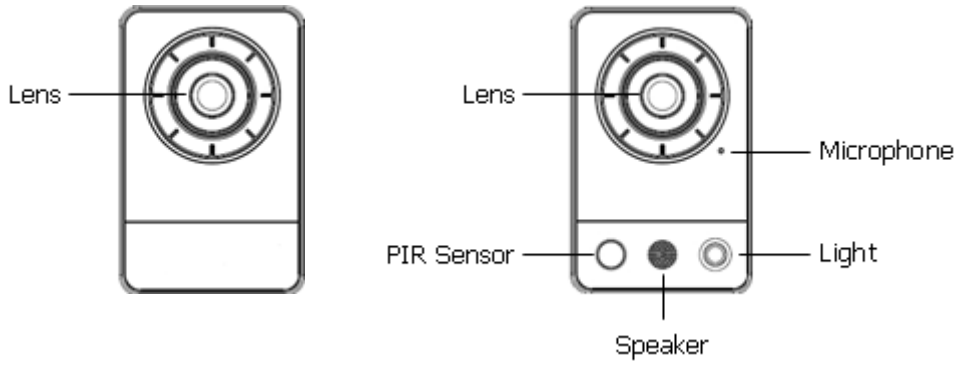
- **PoE (VK2-2MPCCPL)**
  VK2-2MPCCPL can be powered through PoE, which simplifies installation since only one cable is needed for carrying power, as well as video controls.

- **ONVIF**
  This is a global interface standard that makes it easier for end users, integrators, consultants, and manufacturers to take advantage of the possibilities offered by network video technology. ONVIF enables interoperability between different vendor products, increased flexibility, reduced cost, and future-proof systems.

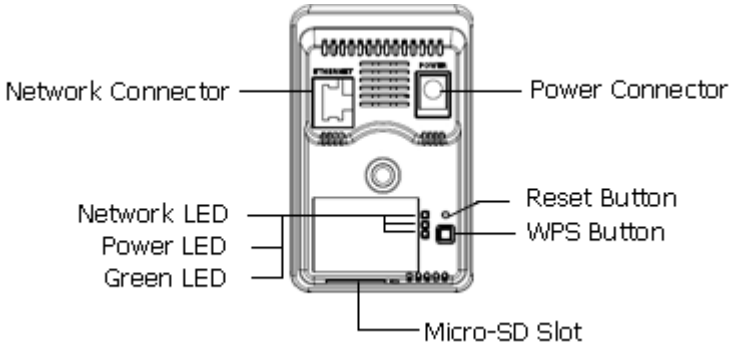
1.3 Overview

- **Front View**

[VK2-2MPCCW] [VK2-2MPCCPL]



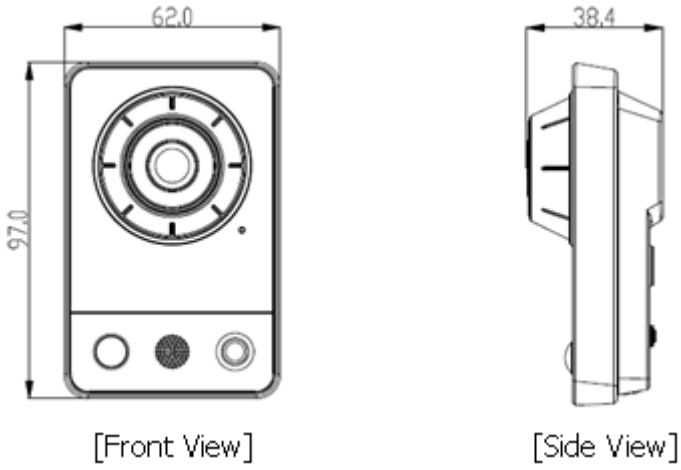
- **Rear View**



NO	Name	Description
1	PIR Sensor	VK2-2MPCCPL is equipped with a PIR Sensor that has a maximum range of 5 meters for detecting movement in the dark.
2	Microphone/Speaker	VK2-2MPCCPL is equipped with a Microphone and Speaker. Two-way audio support allows for remote users to listen in on an area and communicate with visitors or intruders.
3	Light	VK2-2MPCCPL is equipped with White LED that illuminates the scene.
4	Network Connector	Ethernet, RJ-45 port compatible with 10/100Mbps having PoE functionality. Modular Jack
5	Power Connector	For connection of the 5V power adapter (included).
6	Reset Button	Press and hold the Reset Button for one second using a paper clip or thin object. Wait for the camera to reboot.
7	WPS Button	WPS(Wi-Fi Protected Setup) Button, it finds and connects a wireless AP device automatically.
8	Network LED (Green)	Steady for connection to a 100Mbit/s network. Flashes for network activity.
9	Power LED (Green)	Steady green for normal operation or booting. Flashes green during firmware upgrade.
10	Status LED (Red)	Steady red for failed upgrade or booting.

- **Camera Dimension**

See the diagrams below for the exact dimension of the network camera.



[Front View] [Side View]

Dimensions Unit: mm

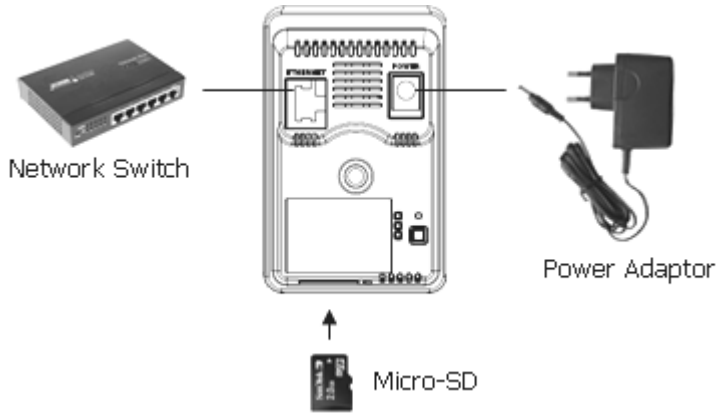
2. INSTALLATION

2.1 Connection

- **Connecting to the RJ-45**
  Connect a standard RJ-45 cable to the network port of the network camera. Generally a cross-over cable is used for directly connection to PC, while a direct cable is used for connection to a hub.

- **Micro SD memory slot**
  Insert the SD memory card.

- **Connecting the Power**
  Connect the supplied DC 5V power adaptor to the camera.



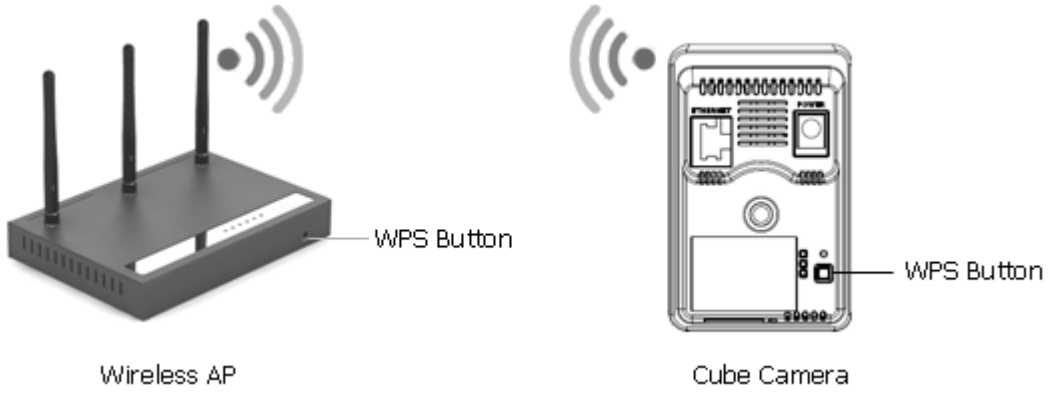
- **Connecting the Wireless using WPS button**

The VK2-2MPCCW supports the wireless function.

Follow steps for a proper operation.

1. Make sure your AP (Access Point) and Operating System support WPS (Wi-Fi Protected Setup) functions. WPS enables easy setup with compatible APs.
2. Press the WPS button on the camera for more 2 seconds. You can then see the Status LED is blinking.
3. Press and hold down the WPS button on your AP (some router/AP will have a virtual button on their management software instead). Refer to your AP's documentation for details using its WPS functions

When WPS configuration is done, wireless connectivity will be established and the security encryption, such as WEP or WPA-PSK, will be synchronized with the AP.
As for IP setting, the camera's use of DHCP or static IP is determined by your configuration on the network camera via the web- based configuration of firmware. The camera's default is DHCP for the VK2-2MPCCW.



Notes:

1. WPS may not work if your AP is configured with a "hidden" SSID.

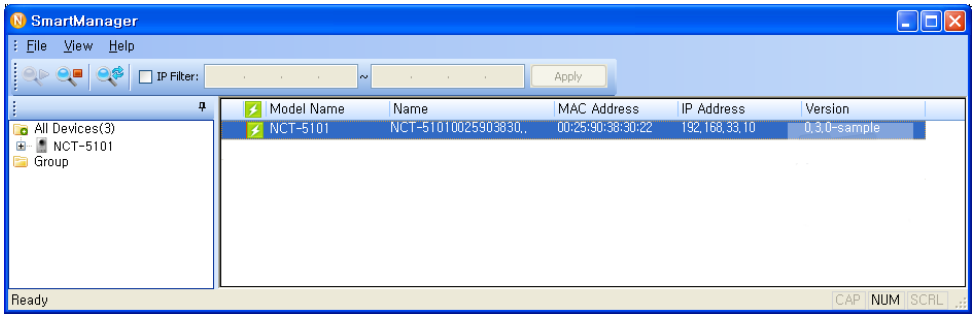
2. If any WPS-enabled AP is not detected, the camera will search APs for 60 seconds after pressing the WPS button, and if the camera still can not detect an AP after 1 minute, the wireless setup will be cancelled.

3. If a camera is assigned with a fixed IP outside the AP's network segment, wireless setup will fail.

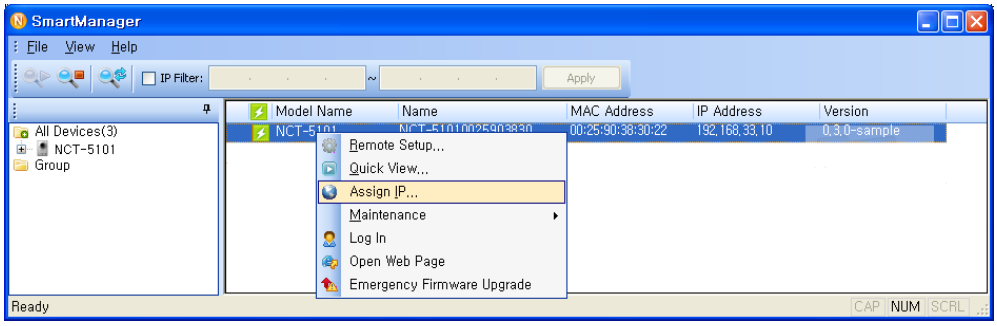
2.2 Network Connection and IP assignment

The Network Camera supports the operation through the network. When a camera is first connected to the network it has no IP address. So, it is necessary to allocate an IP address to the device with the “Smart Manager” utility on the CD. (Default IP 192.168.30.220)

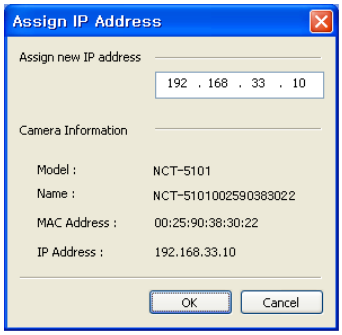
1. Connect the Network Camera / device to the network and power up.
2. Start SmartManager utility (Start>All programs>SmartManager>SmartManager), the main window will be displayed, after a short while any network devices connected to the network will be displayed in the list.



3. Select the camera on the list and click right button of the mouse. You can see the pop-up menu below.



4. Select Assign IP. You cam see a Assign IP window. Enter the required IP address.



Note: For more information, refer to the Smart Manger User’s Manual.

3. OPERATION

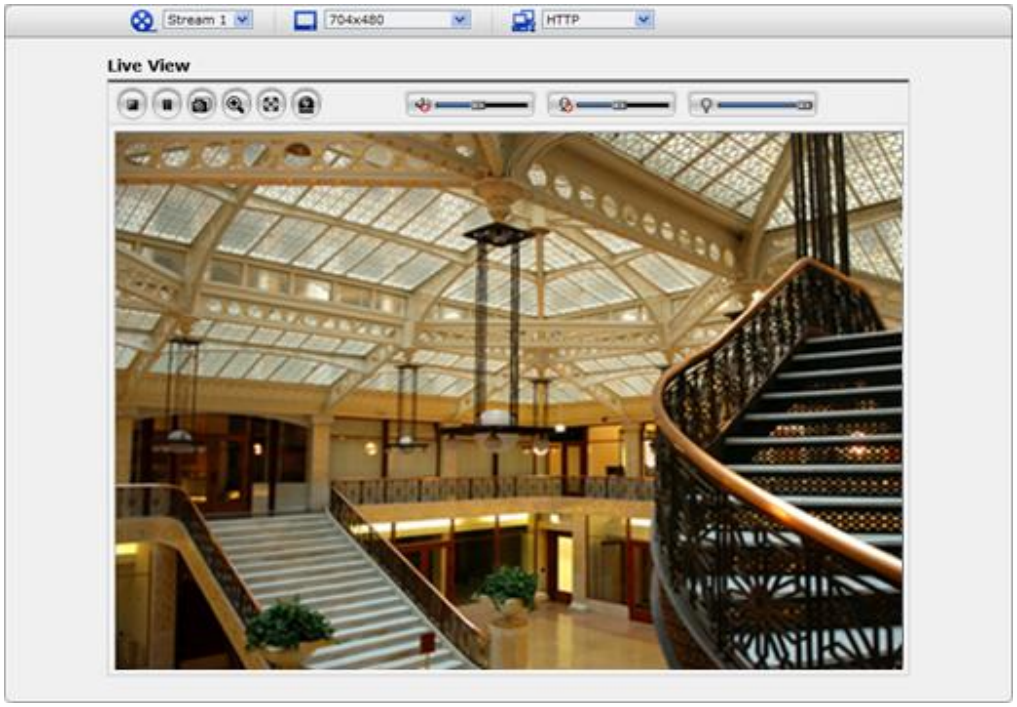
The Network Camera can be used with Windows operating system and browsers. The recommended browsers are Internet Explorer, Safari, Firefox, Opera and Google Chrome with Windows.

NOTE: To view streaming video in Microsoft Internet Explorer, set your browser to allow ActiveX controls.

3.1 Access from a browser

1. Start a browser (Internet Explorer).
2. Enter the IP address or host name of the Network Camera in the Location/Address field of your browser.
3. You can see a starting page. Click Live View or Setup to enter web page.

4. The network camera's **Live View** page appears in your browser.



3.2. Access from the internet

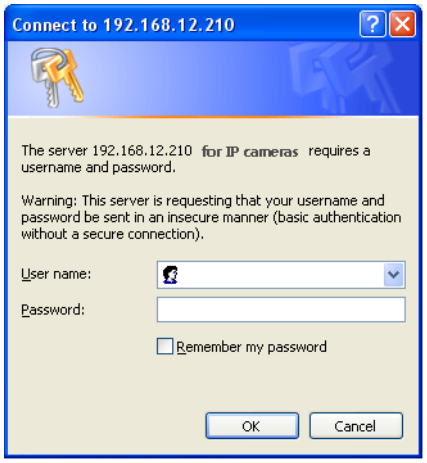
Access from the internet once connected, the Network Camera is accessible on your local network (LAN). To access the network camera from the Internet you must configure your broadband router to allow incoming data traffic to the network camera. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the network camera. This is enabled from Setup > System > Network > NAT.

For more information, please see “3.5.4 System>Network>NAT” of User’s Manual.

3.3 Setting the admin password over a secure connection

To gain access to the product, the password for the default administrator user must be set. This is done in the “Admin Password” dialog, which is displayed when the network camera is accessed for the setup at the first time. Enter your admin name and password, set by the administrator.

Note: The default administrator username and password is “admin”. If the password is lost, the Network Camera must be reset to the factory default settings. See “3.8 Resetting to the Factory Default Settings” for more details.



To prevent network eavesdropping when setting the admin password, this can be done via an encrypted HTTPS connection, which requires an HTTPS certificate (see note below).

To set the password via a standard HTTP connection, enter it directly in the first dialog shown below. To set the password via an encrypted HTTPS connection, see “3.5.6 System >Security>HTTPS”.

Note: HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt the traffic between web browsers and servers. The HTTPS certificate controls the encrypted exchange of information.

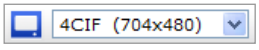
3.4 Live View Page

The live view page comes in several screen modes: 1600x1200, 1280x1024, 1280x720, 800x600, 704x480(576), 640x480, 352x240(288), and 320x240. Users are allowed to select the most suitable one out of those modes. Please, adjust the mode in accordance with your PC specifications and monitoring purposes.

1) General controls

Live View Page Search & Playback Page Setup Page Help Page

The video drop-down list allows you to select a customized or pre-programmed video stream on the live view page. Stream profiles are configured under Setup > Basic Configuration > Video & Image. For more information, please see “3.5.1 Basic Configuration > Video & Image” of User’s Manual.



The resolution drop-down list allows you to select the most suitable one out of video resolutions to be displayed on live view page.

The protocol drop-down list allows you to select which combination of protocols and methods to use depends on your viewing requirements, and on the properties of your network.

2) Control toolbar

The live viewer toolbar is available in the web browser page only. It displays the following buttons:

- The Stop button stops the video stream being played. Pressing the key again toggles the start and stop. The Start button connects to the network camera or start playing a video stream.
- The Pause button pause the video stream being played.
- The Snapshot button takes a snapshot of the current image. The location where the image is saved can be specified.
- The digital zoom activates a zoom-in or zoom-out function for video image on the live screen.

The Full Screen button causes the video image to fill the entire screen area. No other windows will be visible. Press the 'Esc' button on the computer keyboard to cancel full screen view.

The Manual Trigger button activates a pop-up window to manually start or stop the event.

Use this scale to control the volume of the speakers.

Use this scale to control the volume of the microphone.

Use this scale to control the volume of the speakers and microphones.

3) Video Streams

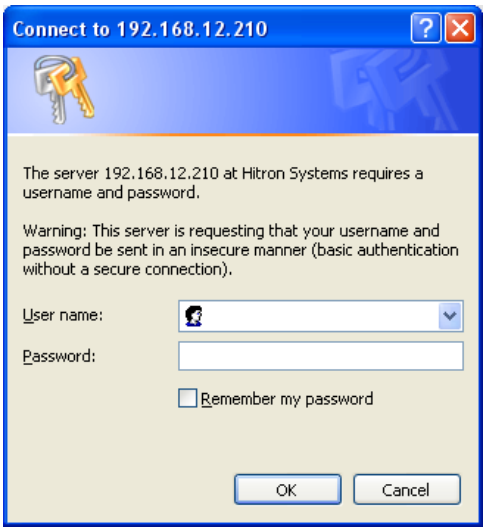
The network camera provides several images and video stream formats. Your requirements and the properties of your network will determine the type you use.

The Live View page in network camera provides access to H.264, MPEG-4 and Motion JPEG video streams, and to the list of available video streams. Other applications and clients can also access these video streams/images directly, without going via the Live View page.

3.5 Network Camera Setup

This section describes how to configure the network camera, and is intended for product Administrators, who have unrestricted access to all the Setup tools; and Operators, who have access to the settings for Basic, Live View, Video & Image, Audio, Event, and System Configuration.

You can configure the network camera by clicking Setup in the top right-hand corner of the Live View page. Click on this page to access the online help that explains the setup tools

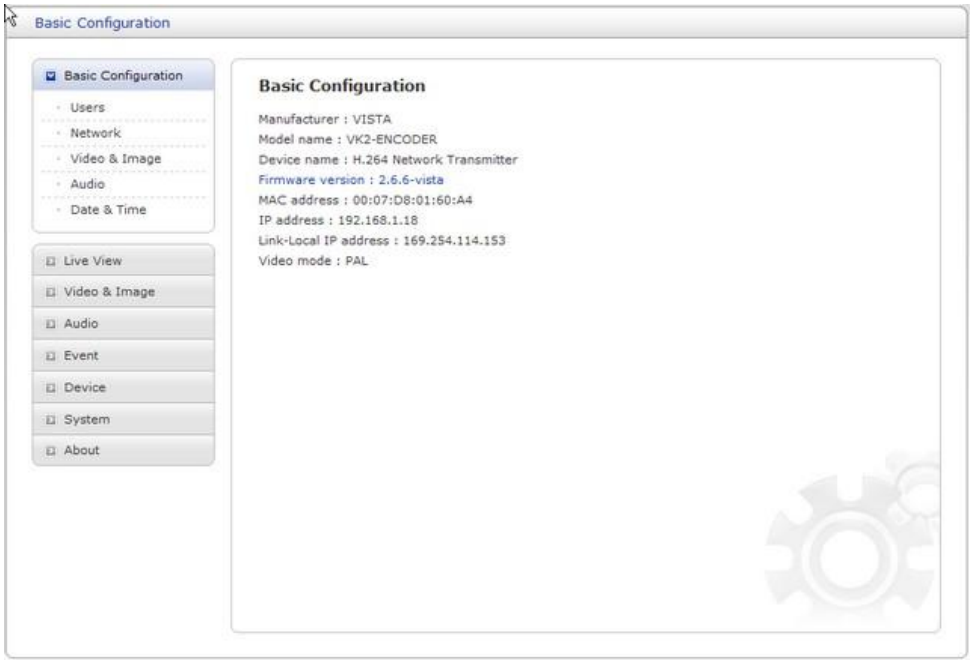


When accessing the Network Camera for the first time, the “Admin Password” dialog appears. Enter your admin name and password, set by the administrator.

Note: If the password is lost, the Network Camera must be reset to the factory default settings. See “3.8 Resetting to the Factory Default Settings”.

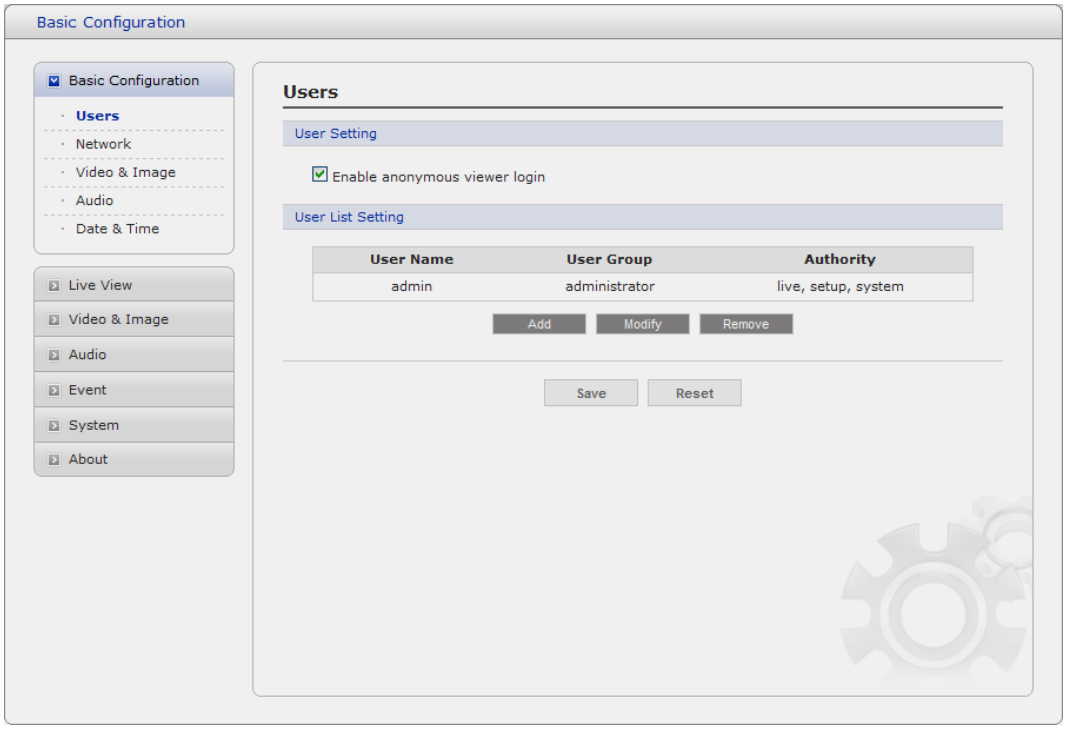
3.5.1 Basic Configuration

You can see the device information in this information page.



1) Users

User access control is enabled by default. An administrator can set up other users, by giving these user names and passwords. It is also possible to allow anonymous viewer login, which means that anybody may access the Live View page, as described below:



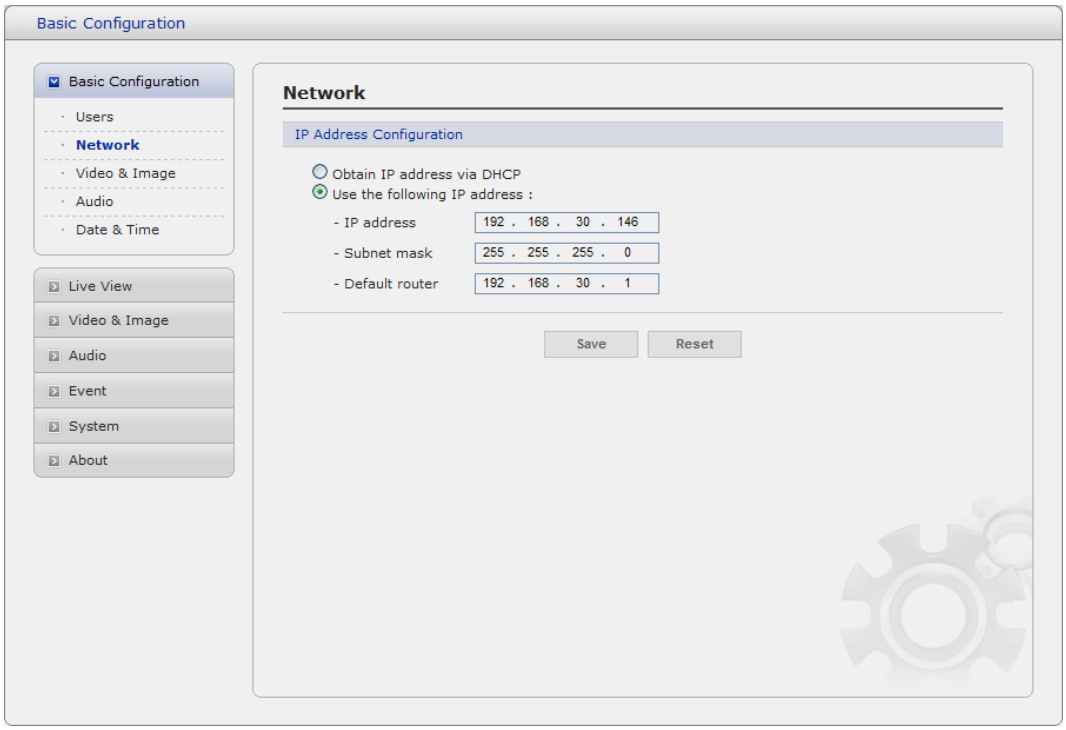
The **user list** displays the authorized users and user groups (levels):

User Group	Authority
Guest	Provides the lowest level of access, which only allows access to the Live View page.
Operator	An operator can view the Live View page, create and modify events, and adjust certain other settings. Operators have no access to System Options.
Administrator	An administrator has unrestricted access to the Setup tools and can determine the registration of all other users.

- **Enable anonymous viewer login:** Check the box to use the webcasting features. Refer to “3.5.2 Video & Image” for more details.

2) Network

The network camera supports both IP version 4 and IP version 6. Both versions may be enabled simultaneously, and at least one version must always be enabled. When using IPv4, the IP address for the network camera can be set automatically via DHCP, or a static IP address can be set manually. If IPv6 is enabled, the network camera receive an IP address according to the configuration in the network router. There is also the option of using the Internet Dynamic DNS Service. For more information on setting the Network, please see Setup> System>Security>Network.



- **Obtain IP address via DHCP** - Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address.

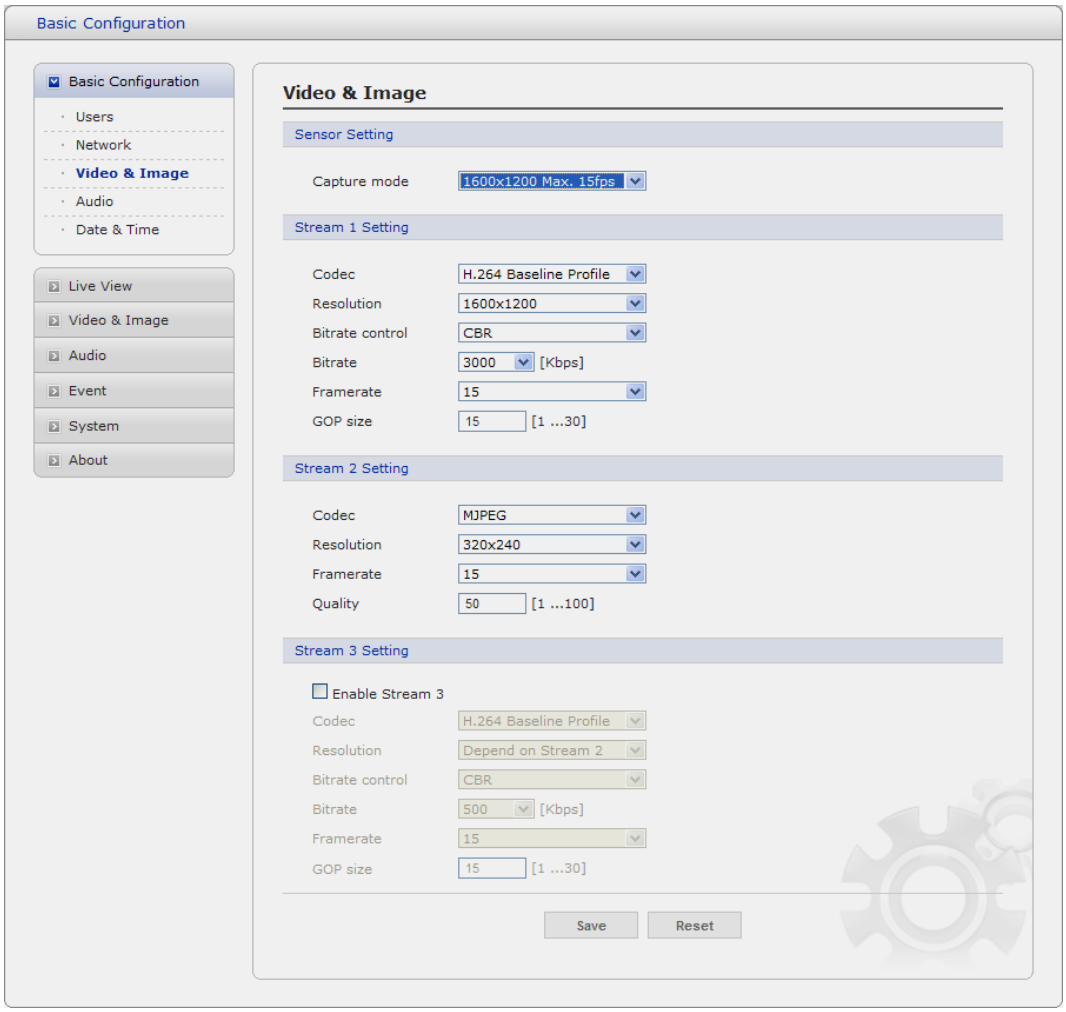
- **Use the following IP address** - To use a static IP address for the Network Camera, check the radio button and then make the following settings:
  - **IP address** - Specify a unique IP address for your Network Camera.
  - **Subnet mask** - Specify the mask for the subnet the Network Camera is located on.
  - **Default router** - Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

Notes:

1. DHCP should only be enabled if using dynamic IP address notification, or if your DHCP server can update a DNS server, which then allows you to access the Network Camera by name (host name). If DHCP is enabled and you cannot access the unit, you may have to reset it to the factory default settings and then perform the installation again.
2. The ARP/Ping service is automatically disabled two minutes after the unit is started, or as soon as an IP address is set.

3. Pinging the unit is still possible when this service is disabled.

3) Video & Image



- **Sensor Setting**
  - **Capture Mode:**

    Choose Capture Mode you wish to use from the drop-down list:

  * **1600x1200 Max 15fps:** Capture resolution is 1600x1200 and Maximum frame is 15.
  * **1280x720 Max 30fps:** Capture resolution is 1280x720 and Maximum frame is 30.
  * **800x600 Max 30fps:** Capture resolution is 800x600 and Maximum frame is 30.

  Note: Maximum frame rate for each Stream is restricted under the one of the Capture Mode.

- **Stream1 Setting**
  - **Codec:**

    The codec settings are separated into MPEG4 and H.264.

    H.264 is also known as MPEG-4 Part 10. This is the new generation compression standard for digital video. This function offers higher video resolution than Motion JPEG or MPEG-4 at the same bit rate and bandwidth, or the same quality video at a lower bit rate.

  - **Profile:**

    There are 4 pre-programmed stream profiles available for quick set-up.

Choose the form of video encoding you wish to use from the drop-down list:

* **H.264 MP(Main Profile):**
  Primarily for low-cost applications that requires additional error robustness, this profile is used rarely in videoconferencing and mobile applications, it does add additional error resilience tools to the Constrained Baseline Profile. The importance of this profile is fading after the Constrained Baseline Profile has been defined.
* **H.264 BP(Base Profile):**
  Originally intended as the mainstream consumer profile for broadcast and storage applications, the importance of this profile faded when the High profile was developed for those applications.
* **MPEG4 SP(Simple Profile):**
  Mostly aimed for use in situations where low bit rate and low resolution are mandated by other conditions of the applications, like network bandwidth, device size etc.

- **Resolution:**
  It enables users to determine a basic screen size when having an access through the Web Browser or PC program. The screen size control comes in seven modes like 1600x1200, 1280x1024, 1280x720, 800x600, 640x480, 352x240, and 320x240. Users can reset the selected screen size anytime while monitoring the screen on a real-time basis.

- **Bitrate control:**
  Limiting the maximum bit rate helps control the bandwidth used by the H.264 or MPEG-4 video stream. Leaving the Maximum bit rate as unlimited maintains consistently good image quality but increases bandwidth usage when there is more activity in the image. Limiting the bit rate to a defined value prevents excessive bandwidth usage, but images are lost when the limit is exceeded.
  Note that the maximum bit rate can be used for both variable and constant bit rates.

  The bit rate can be set as Variable Bit Rate (VBR) or Constant Bit Rate (CBR). VBR adjusts the bit rate according to the image complexity, using up bandwidth for increased activity in the image, and less for lower activity in the monitored area.

  CBR allows you to set a fixed target bitrate that consumes a predictable amount of bandwidth. As the bit rate would usually need to increase for increased image activity, but in this case cannot, the frame rate and image quality are affected negatively. To partly compensate for this, it is possible to prioritize either the frame rate or the image quality whenever the bit rate needs to be increased. Not setting a priority means the frame rate and image quality are equally affected.

- **Frame rate:**
  Upon the real-time play, users should select a frame refresh rate per second. If the rate is high, the image will become smooth. On the other hand, if the rate is low, the image will not be natural but it can reduce a network load.

- **GOP size:**
  Select the GOP(Group of Picture) size. If users want to have a high quality of fast image one by one, please decrease the value. For the purpose of general monitoring, please do not change a basic value. Such act may cause a problem to the system performance. For the details of GOP setting, please contact the service center.

- **Stream2 Setting**

  Sometimes the image size is large due to low light or complex scenery. Adjusting the frame rate and quality helps to control the bandwidth and storage used by the Motion JPEG video stream in these situations. Limiting the frame rate and quality optimizes bandwidth and storage usage, but may give poor image quality. To prevent increased bandwidth and storage usage, the Resolution, Frame rate, and Frame Quality should be set to an optimal value.

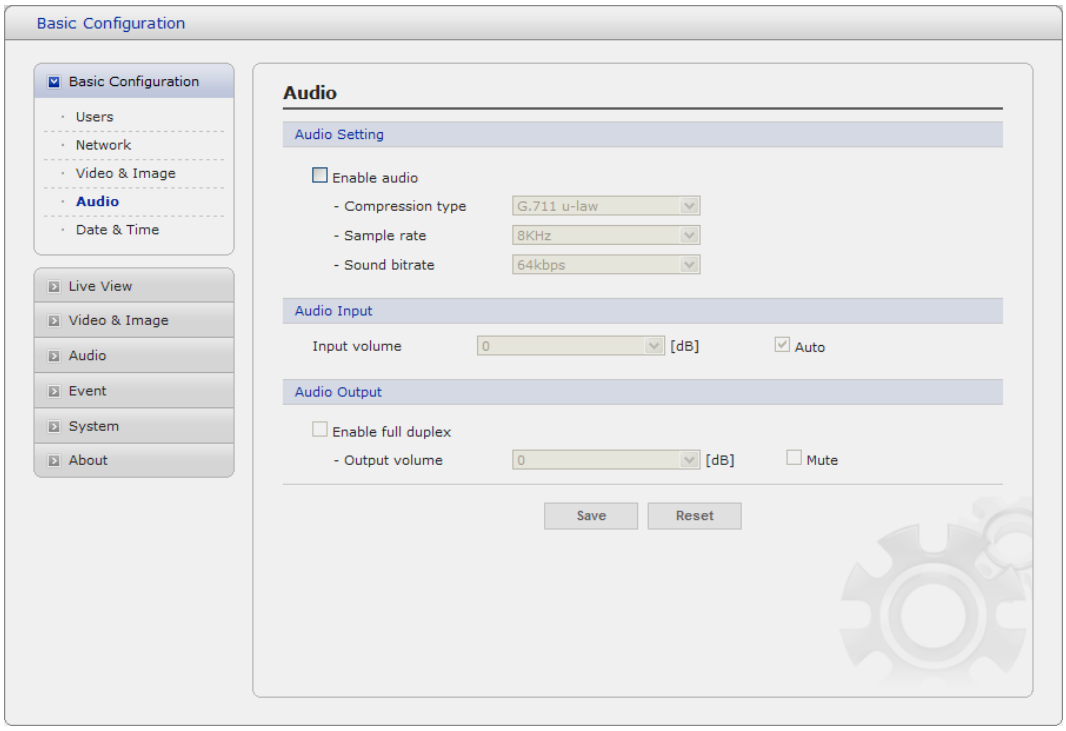
  - **JPEG resolution:** Same as the Stream1 Setting.
  - **JPEG frame rate:** Same as the Stream1 Setting.
  - **JPEG quality:** Select the picture quality. If users want to have a high quality of fast image one by one, please decrease the value. For the purpose of general monitoring, please do not change a basic value. Such act may cause a problem to the system performance.

- **Stream3 Setting**

  Same as the Stream1 Setting. Click the checkbox to activate the 3rd stream.

When satisfied with the settings, click **Save**, or click **Reset** to revert to previously saved settings.

4) Audio



The Network Camera can transmit audio to other clients using an external microphone and can play audio received from other clients by attaching a speaker. The Setup page has an additional menu item called **Audio**, which allows different audio configurations, such as, full duplex, and simplex.

- **Audio Setting**
  - **Enable audio:**
    Check the box to enable audio in the video stream.
  - **Compression type:**
    Select the desired audio Compression format, G711.
  - **Sample rate:**
    Select the required Sample rate (number of times per second the sound is sampled). The higher the sample rate, the better the audio quality and the greater the bandwidth required.
  - **Sound bitrate:**
    Depending on the selected encoding, set the desired audio quality (bitrate). The settings affect the available bandwidth and the required audio quality.

- **Audio Input**
  Audio from an external line source can be connected to the terminal I/O of the network camera.
  - **Input volume:**
    If there are problems with the sound input being too low or high, it is possible to adjust the input gain for the microphone attached to the network camera.

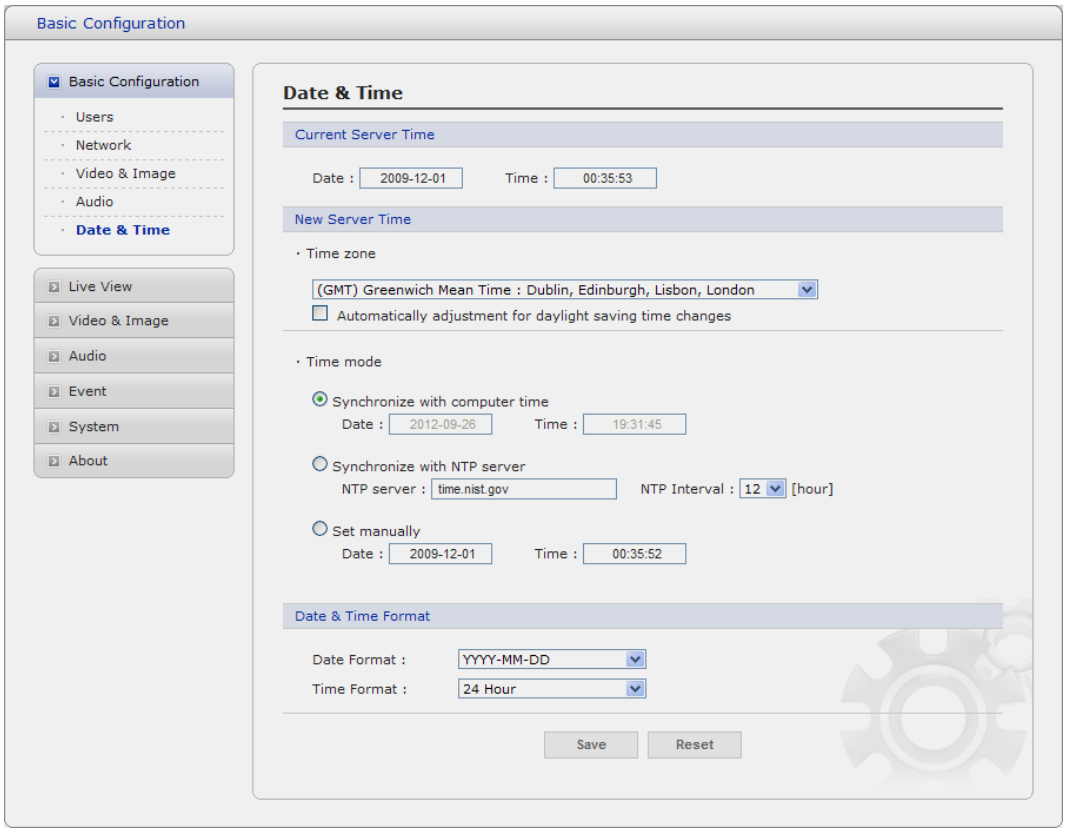
- **Audio Output**
  - **Enable full duplex:**
    Check the box to enable Full Duplex mode. It means that you can transmit and receive audio (talk and listen) at the same time, without having to use any of the controls. This is just like having a telephone conversation.
    This mode requires that the client PC has a sound card with support for full-duplex audio.

    Uncheck the box enable Simplex mode. The simplex mode only transmits audio from the network camera to any web client. It does not receive audio from other web clients.

  - **Output volume:**
    If the sound from the speaker is too low or high it is possible to adjust the output gain for the active speaker attached to the network camera.

  When satisfied with the settings, click **Save**, or click **Reset** to revert to previously saved settings

5) Date & Time



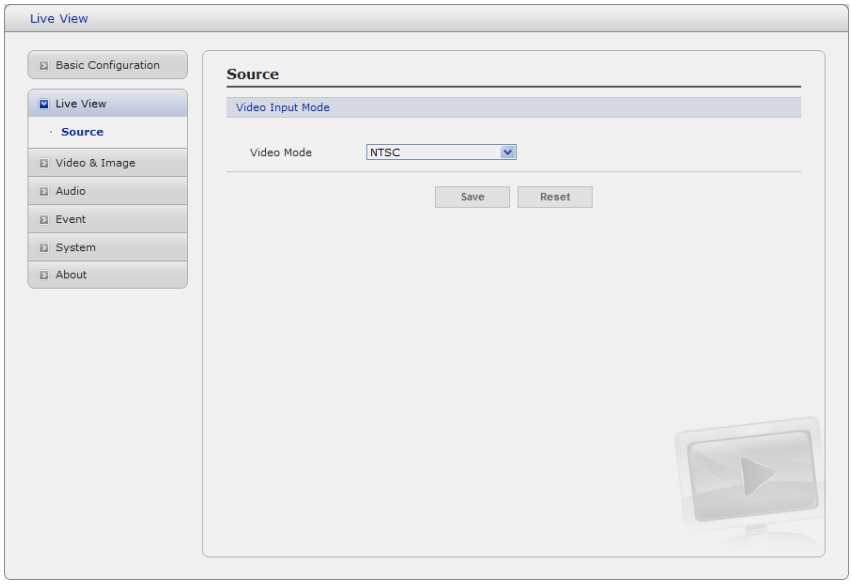
- **Current Server Time**
  It displays the current date and time (24h clock). The time can be displayed in 12h clock format in the overlay (see below).
- **New Server Time**
  Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, select the “Automatically adjustment for daylight saving time changes”.

  From the **Time Mode** section, select the preferred method to use for setting the time:
  - **Synchronize with computer time:** sets the time from the clock on your computer.
  - **Synchronize with NTP Server:** the network camera will obtain the time from an NTP server every 60 minutes.
  - **Set manually:** this option allows you to manually set the time and date.

- **Date & Time Format**
  Specify the formats for the date and time (12h or 24h) displayed in the video streams.
  Select Date & Time format from the drop-down list.
  - **Date Format:** Specify the date format. YYYY: Year, MM: Month, DD: Day
  - **Time Format:** Specify the date format. 24Hours or 12 Hours

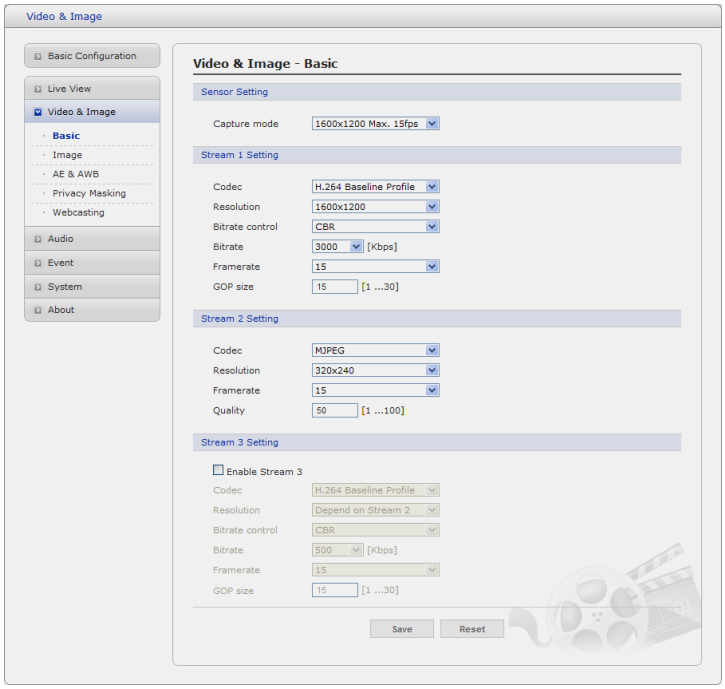
3.5.2 Video & Image

▼ Live View



- **Video Input Mode**
  - **Video Mode:**
    Choose Video Mode you wish to use from the drop-down list: NTSC or PAL

▼ Basic



Refer to “3.5.1 Basic Configuration > Video & Image” for more details.

▼ Image

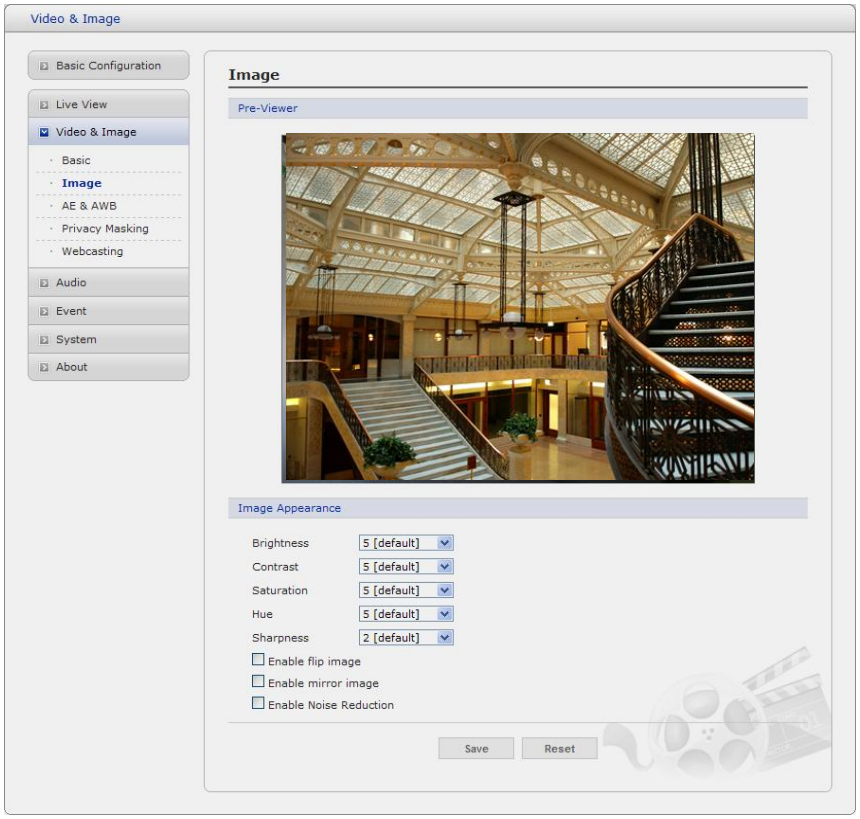
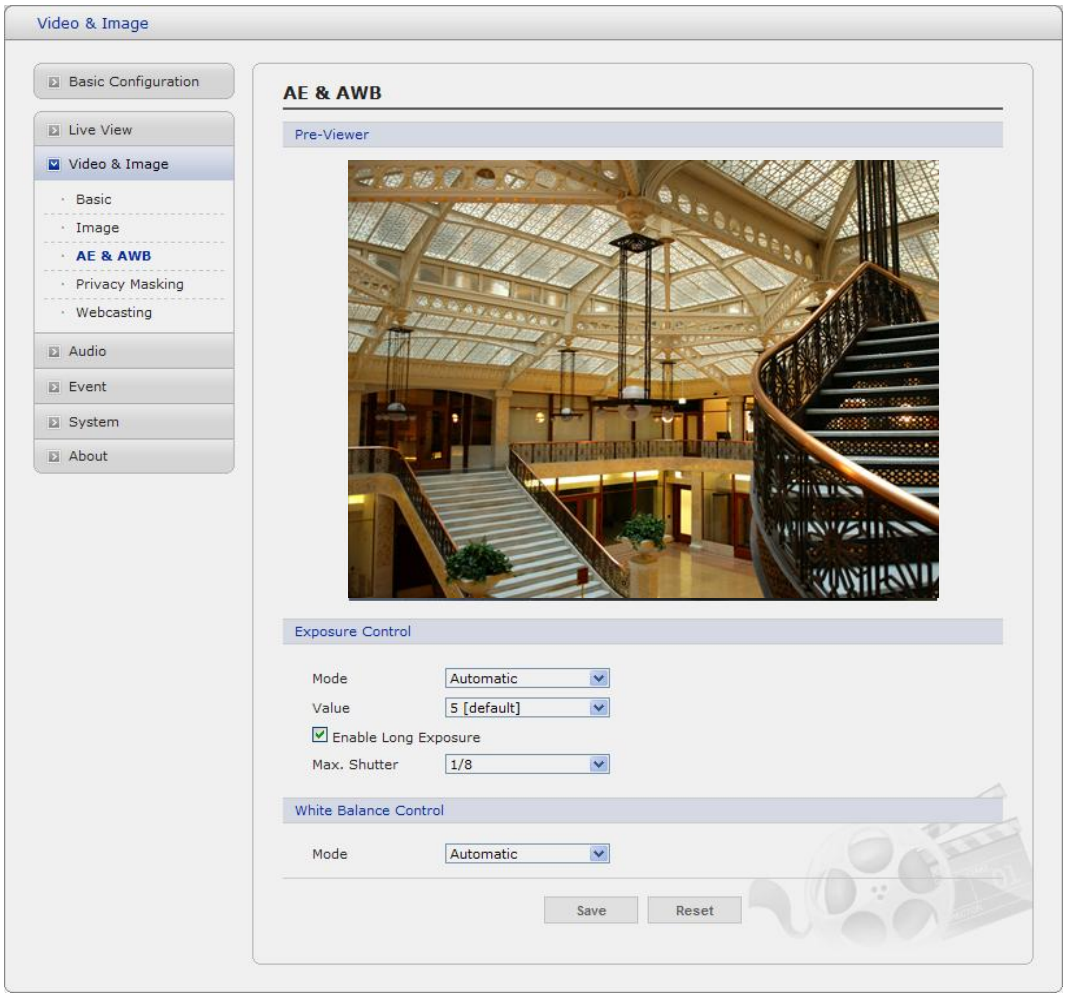


Image Appearance

This page provides access to the advanced image settings for the network camera.

- **Brightness:** The image brightness can be adjusted in the range 1-10, where a higher value produces a brighter image.
- **Contrast:** Adjust the image's contrast by raising or lowering the value in this field.
- **Saturation:** Select an appropriate level by entering a value in the range 1-10. Lower values mean less color saturation.
- **Sharpness:** Controls the amount of sharpening applied to the image. A sharper image might increase image noise especially in low light conditions. A lower setting reduces image noise, but the image would be less sharp.
- **Enable flip image:** Check this box to flip the image.
- **Enable mirror image:** Check this box to mirror the image.
- **Enable Noise Reduction:** Check this box to reduce an image noise.

▼ AE & AWB



This page provides access to set the exposure and white balance of the network camera.

- **Exposure Control**

  Configure the exposure settings to suit the image quality requirements in relation to lighting consideration.

  - **Mode:** Supports exposure modes to control the amount of light detected by the camera sensor based on settings for light conditions. The default setting is Auto with DC-IRIS.
  * **Automatic:** Automatically sets the amount of light detected by the DC-IRIS and AGC.
  * **Hold Current:** Fixes the exposure at its current state.
  - **Value:** Select a value in the drop-down list to tune the exposure. The default setting is 5.
  - **Enable Long Exposure:** Set this checkbox to activate the electronic shutter of the camera.
  * Max. Shutter: Select a shutter speed value in the drop-down list. The default setting is 1/8.

- **White Balance Control**

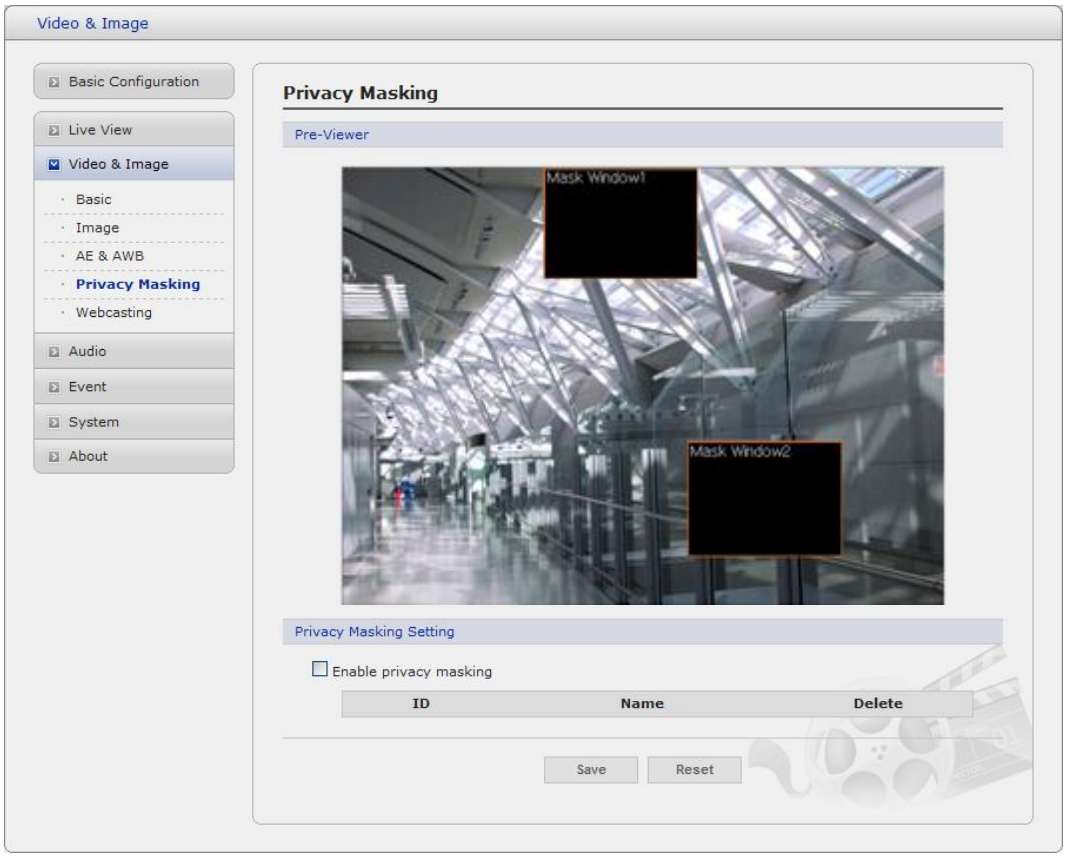
  This adjusts the relative amount of red, green and blue primary colors in the image so that the neutral colors are reproduced correctly. The camera can be set to automatically adjust for the type of light and compensate for its color. Alternatively, the type of light source can be set manually.
  From the drop-down list, select the white balance setting suitable for the lighting used for your

camera. The available options are:

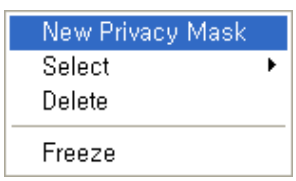
- **Automatic:** Automatic identification and compensation for the light source color. This can be used in most situations and is the recommended setting.
- **Fixed Incandescent:** Fixed color adjustment, ideal for a room with incandescent (a glow) lighting and good for a normal color temperature around 2600K.
- **Fixed Fluorescent:** Fixed color adjustment; good for fluorescent lighting with a color temperature around 4000K to 5000K.
- **Fixed Outdoor:** Fixed color adjustment for sunny, with a color temperature around 6500K to 7500K.

▼ Privacy Masking

The privacy masking function allows you to mask parts of the video image to be transmitted. You can set up to eight privacy masks and the color of privacy masks is black.



The privacy masks are configured by Mask windows. Each window can be selected by clicking with the mouse. It is also possible to **resize or delete, or move** the window, by selecting the appropriate window at the mouse menu on the video screen.



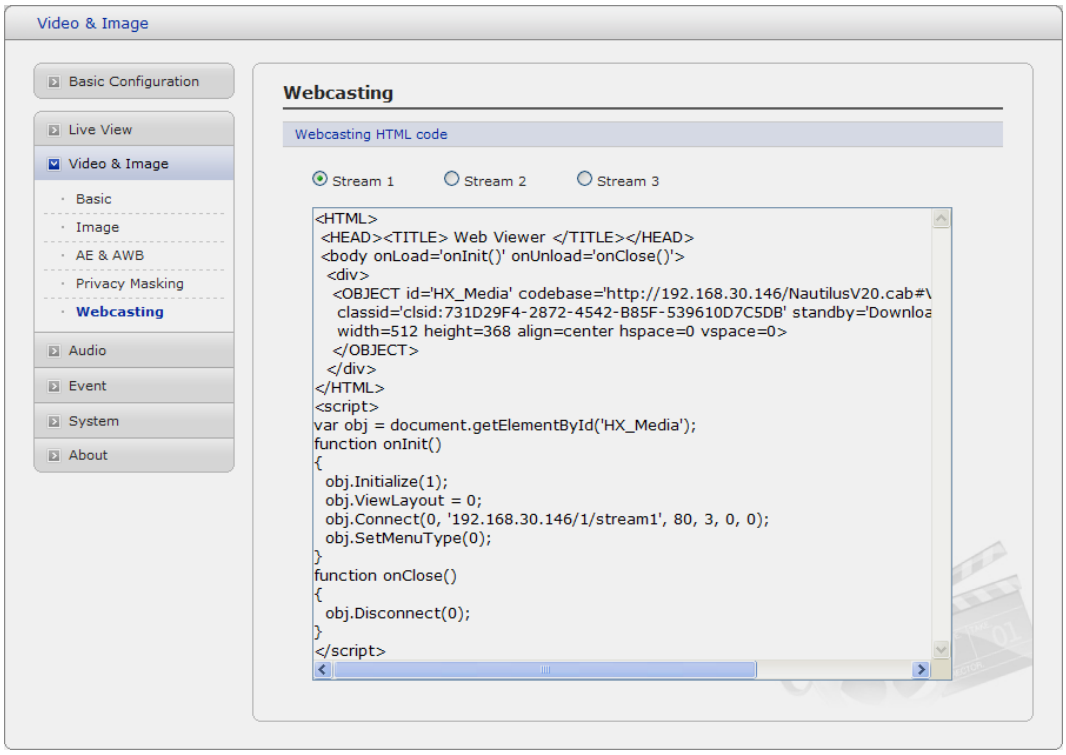
To create a mask window, follow steps:

1. Click the right button of mouse to see the mouse menu.
2. Select New Privacy Mask in the mouse menu.
3. Click and drag mouse to designate a mask window area.

You can also modify or delete a mask window index. Select an index and then, modify items or delete button. Select “Enable” to activate the privacy masking function.

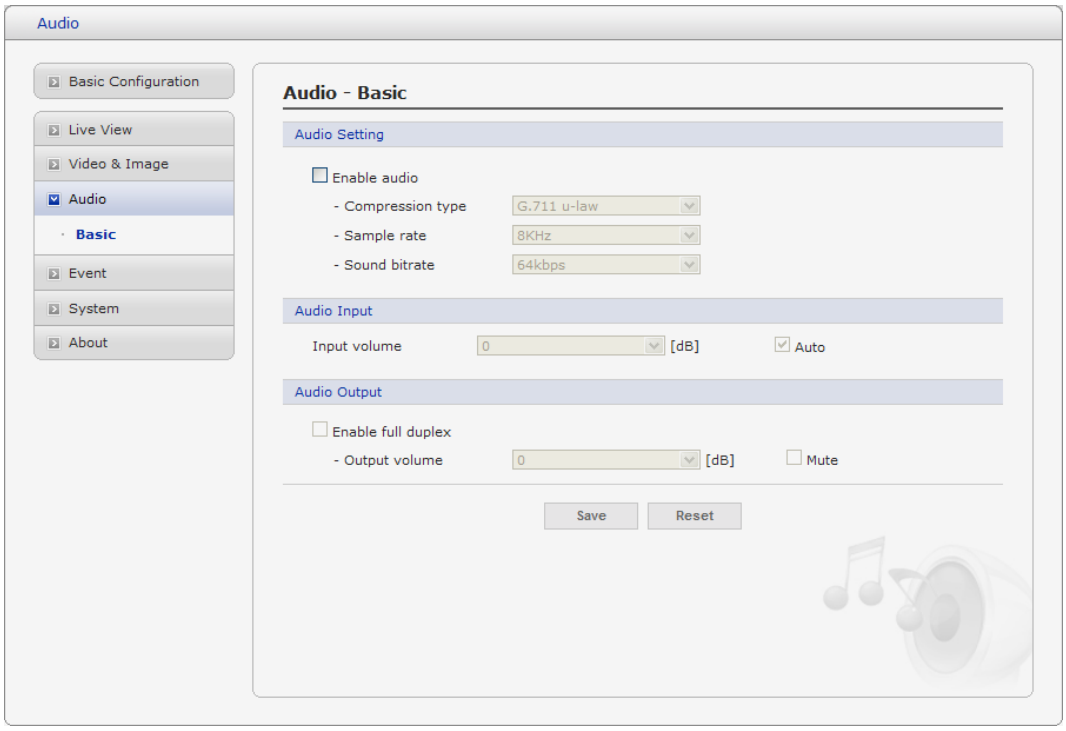
▼ Webcasting

The network camera can stream live video to a website. Copy the HTML code generated on the screen and pastes it in page code of the website you want to display live video.



Note: To use webcasting service, the Enable Anonymous viewer login option must be checked. Refer to “3.5.1 Basic Configuration > Users” for more details.

3.5.3 Audio

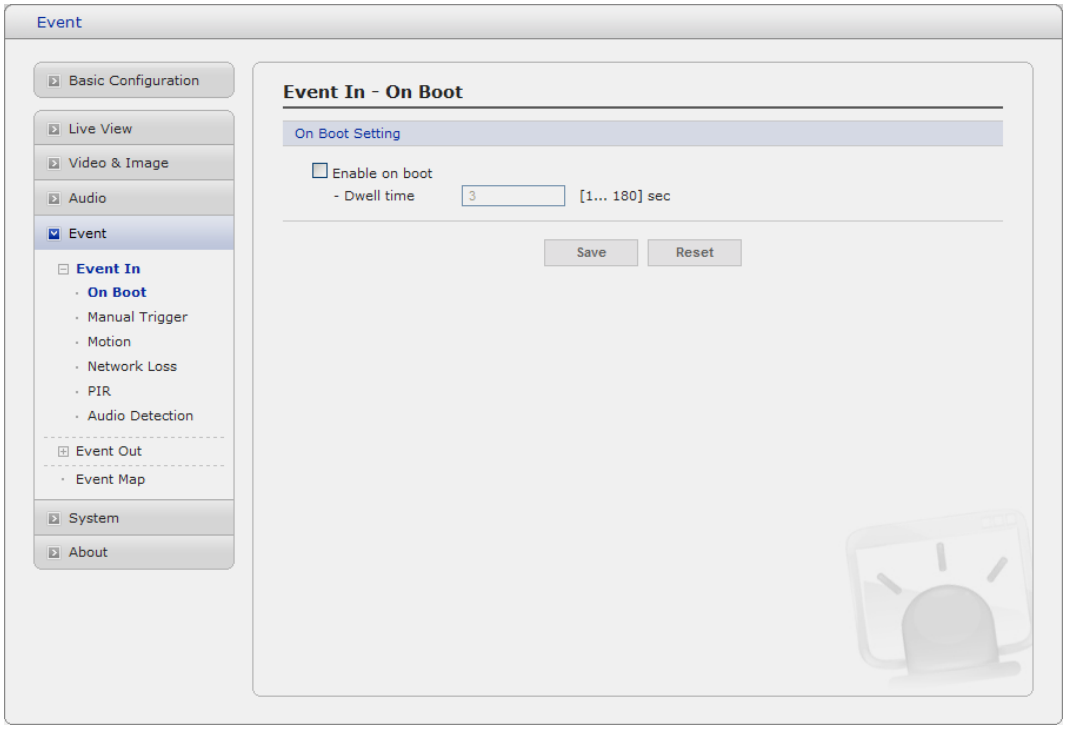


Refer to “3.5.1 Basic Configuration > Audio” for more details.

3.5.4 Event

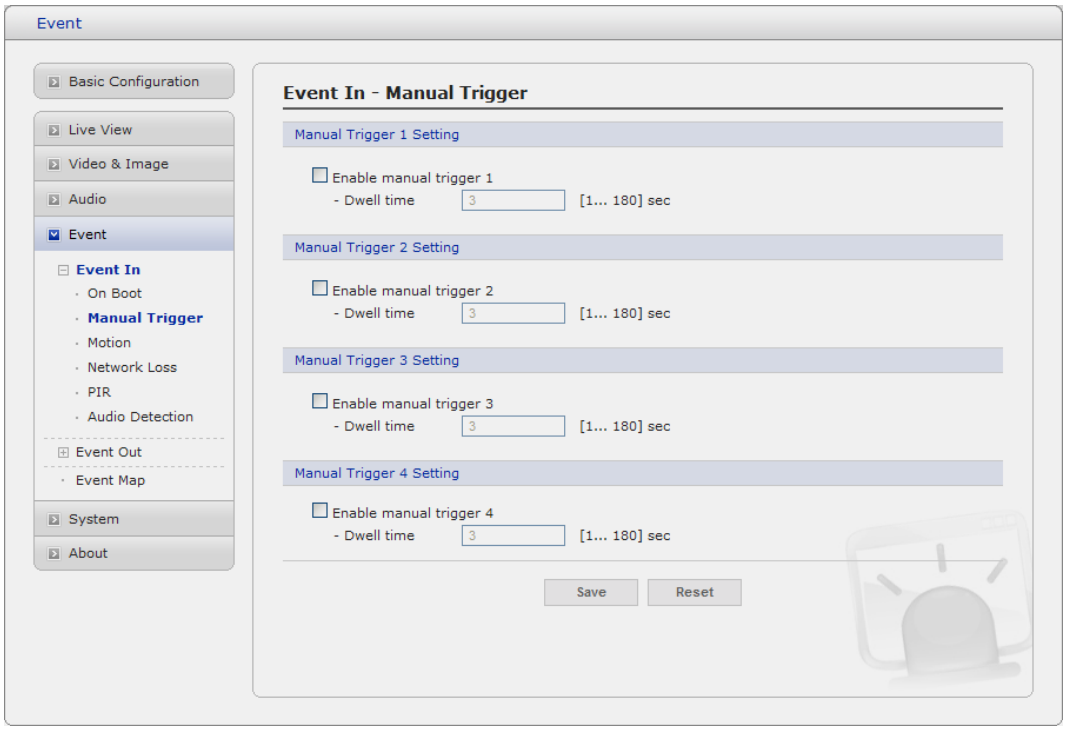
1) Event-In

▼ On Boot



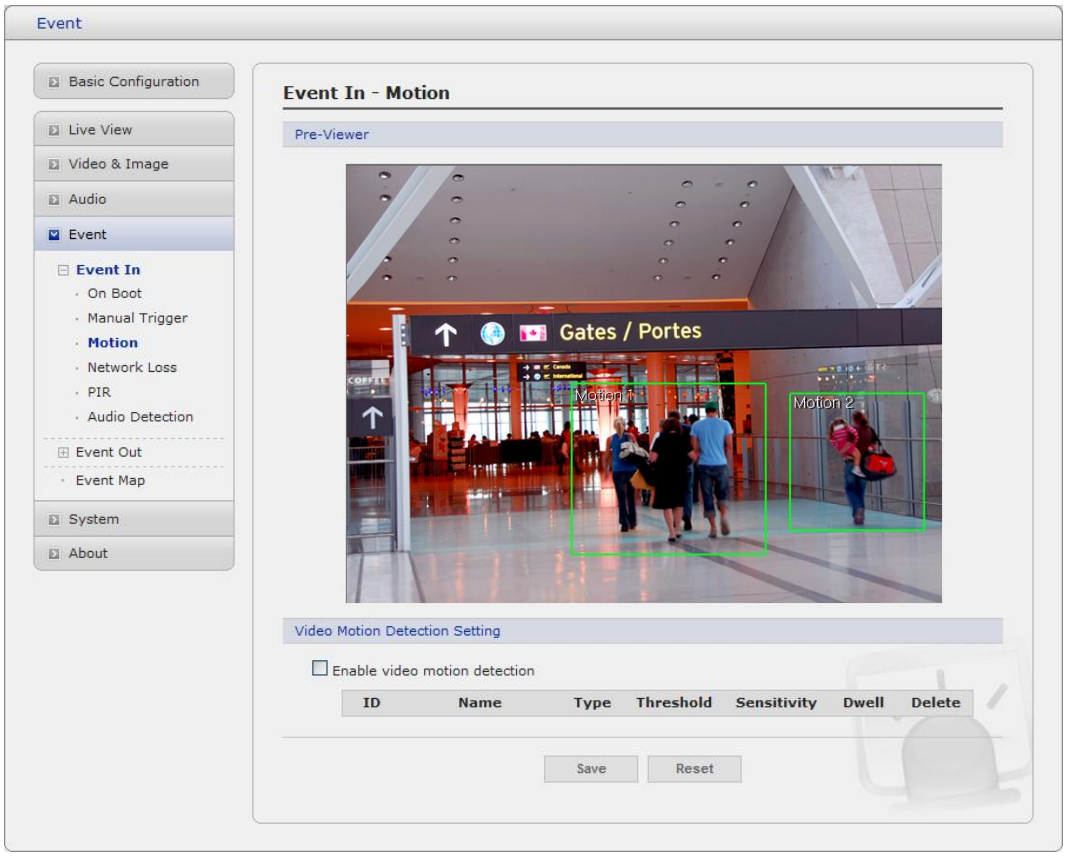
This is used to trigger the event every time the Network Camera is started. Select “Enable” to activate the motion event.

▼ Manual Trigger



This option makes use of the manual trigger button provided on the live view page, which are used to start or stop the event type manually. Alternatively the event can be triggered via the product's API (Application Programming Interface).

▼ Motion



Motion detection is used to generate an alarm whenever movement occurs (or stops) in the video image. A total of 8 Motion and/or Mask windows can be created and configured.

Motion is detected in defined **Motion** windows, which are placed in the video image to target specific areas. Movement in the areas outside the motion windows will be ignored. If part of a motion window needs to be masked, this can be configured in a **Mask** window.

- **Pre-Viewer**
  Motion detection windows are configured by Motion or Mask windows. Each window can be selected by clicking with the mouse. It is also possible to **resize or delete, or move** the window, by selecting the appropriate window at the mouse menu on the video screen.

To create a motion or mask window, follow steps:

1. Click the right button of mouse to see the mouse menu.
2. Select New Motion (or Mask) Window in the mouse menu.
3. Click and drag mouse to designate a motion area.

- **Motion Detection Setting**
  The behavior for each window is defined by adjusting the Threshold and Sensitivity, as described below.

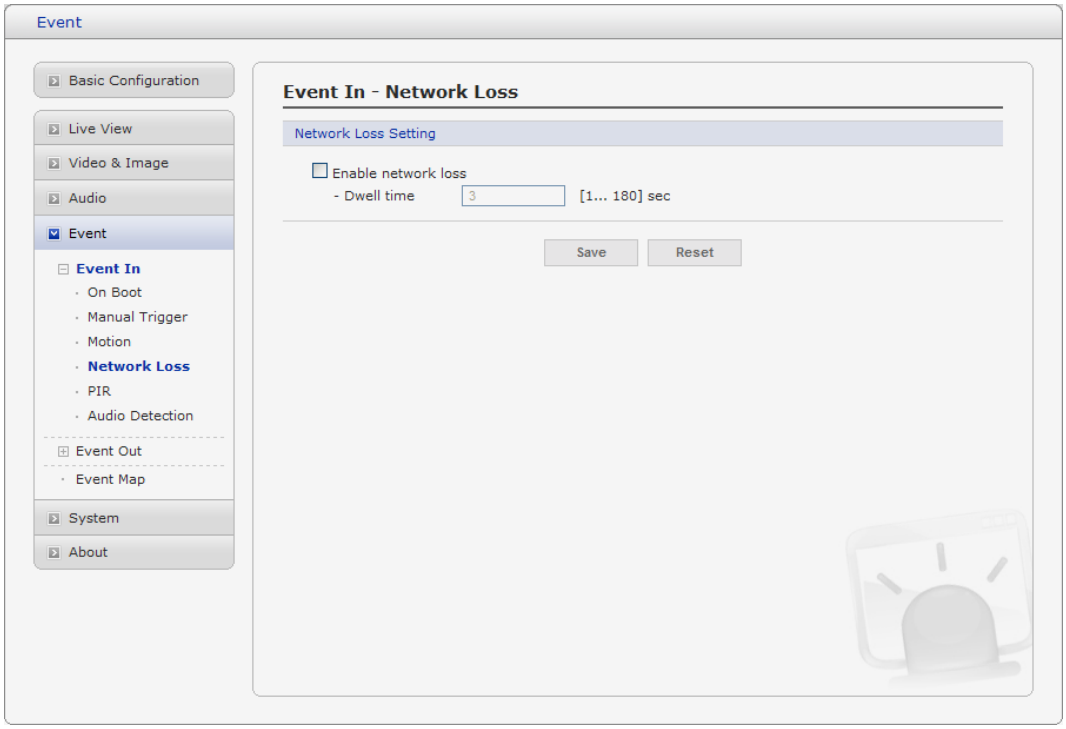
  A motion index is a set of parameters describing Window Name, Type, Threshold, Sensitivity, and Dwell Time. Window Types is one of Motion and Mask windows.

  - **Threshold:** Sets up the threshold for the motion detection.
  - **Sensitivity:** Sets up the sensitivity for the motion detection.
  - **Dwell Time:** Set the hold time an event lasts for the specified hold time from the point of detection of a motion.

You can also modify or delete a motion index. Select an index and then, click the Modify or Delete button.

Select “Enable” to activate the motion window.

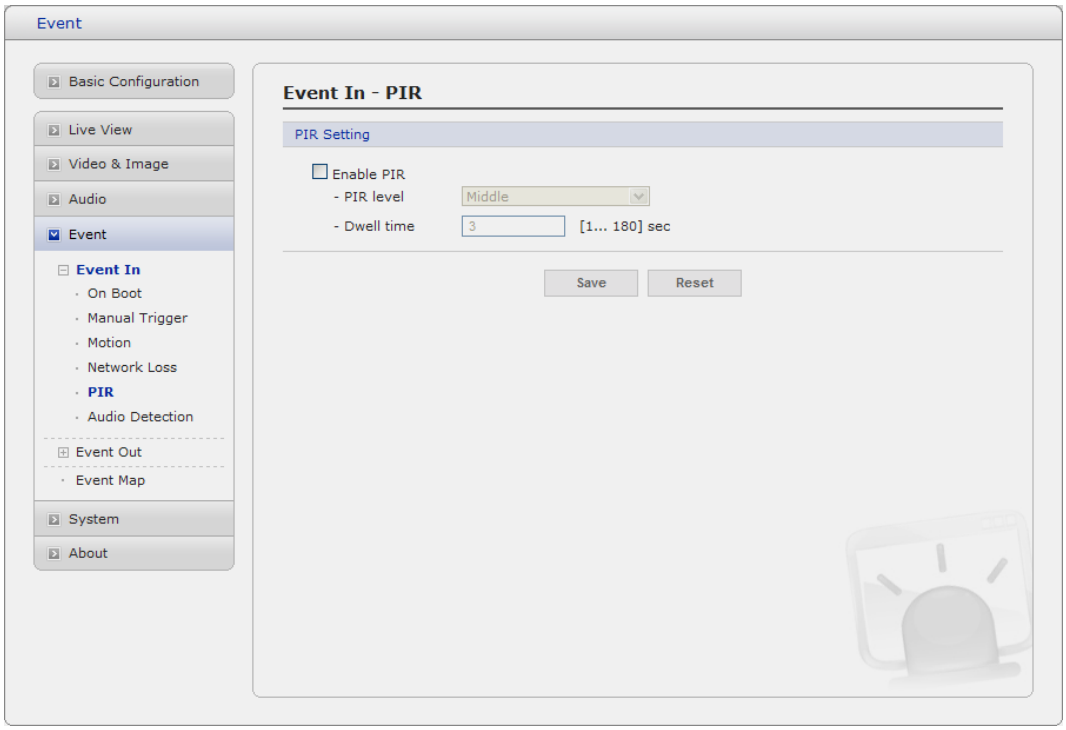
▼ Network Loss



This is used to trigger the event every time the network connection is failed. Select “Enable” to activate the Network Loss event.

▼ PIR

The VK2-2MPCCPL is also able to detect motion using the PIR Sensor. Since the PIR Sensor can detect a moving infrared object such as a person in the dark, it can be used as an intruder alarm when, for example, a thief tries to break into a building at night.



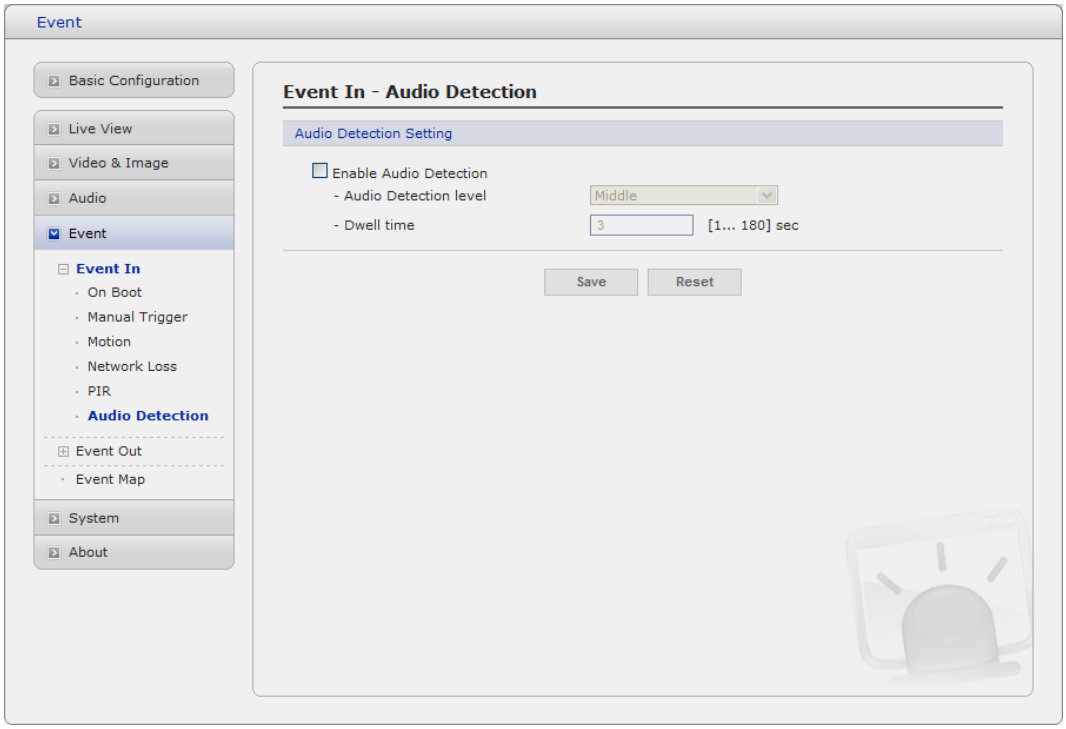
- **PIR Setting**
  Select the sensitivity from the drop-down menu.

  - **PIR Level:** Be used to adjust the sensitivity of the PIR Sensor from 10-100%. The default level is 50%.
  - **Dwell Time:** Set the hold time an event lasts for the specified hold time from the point of detection of the PIR sensor.

  Select “Enable” to activate the PIR Sensor.

▼ Audio Detection

The VK2-2MPCCPL is also able to detect change of the ambient voice using a built-in microphone.



Audio detection can be used to measure change in the ambient voice.

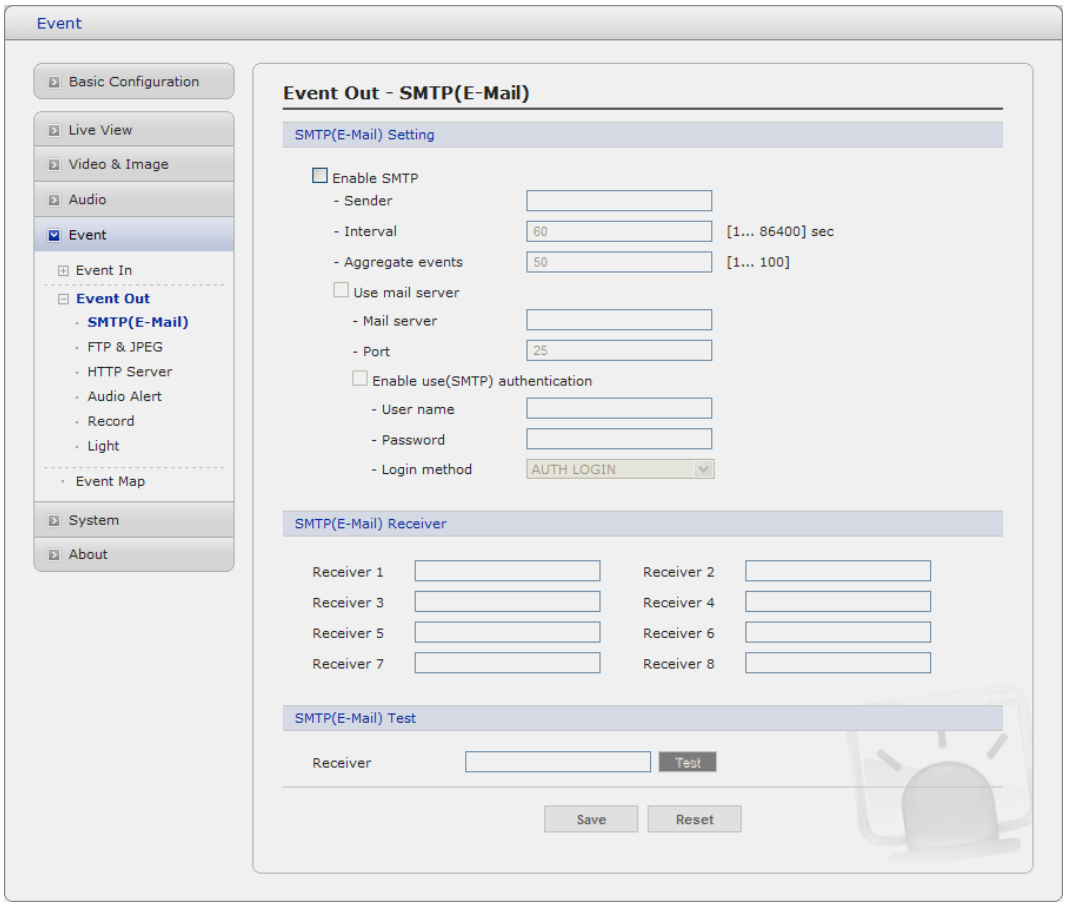
- **Audio Detection Setting**
  Select the sensitivity from the drop-down menu.

  - **Audio Detection Level:** Be used to adjust the sensitivity of the audio level from 10-100%. The default level is 50%.
  - **Dwell Time:** Set the hold time an event lasts for the specified hold time from the point of detection of the audio level.

  Select “Enable” to activate the Audio Detection.

2) Event-Out

▼ SMTP(E-Mail)



The Network Camera can be configured to send event and error email messages via SMTP (Simple Mail Transfer Protocol).

- **SMTP(E-Mail) Setting**
  Select “Enable” to activate the SMTP operation.
  - **Mail Server / Port:** Enter the host names (or IP addresses) and port numbers for your mail server in the fields provided, to enable the sending of notifications and image email messages from the camera to predefined addresses via SMTP.
  - **Sender:** Enter the email address to be used as the sender for all messages sent by the Network Camera.
  - **Interval:** Represents the frequency of the email notification when an event occurs.
  - **Aggregate events:** Shows the maximum number of emails sent within each interval.

  If your mail server requires authentication, check the box for Use authentication to log in to this server and enter the necessary information.
  - **User Name/Password:** Enter the User Name and Password as provided by your network administrator or ISP (Internet Service Provider).

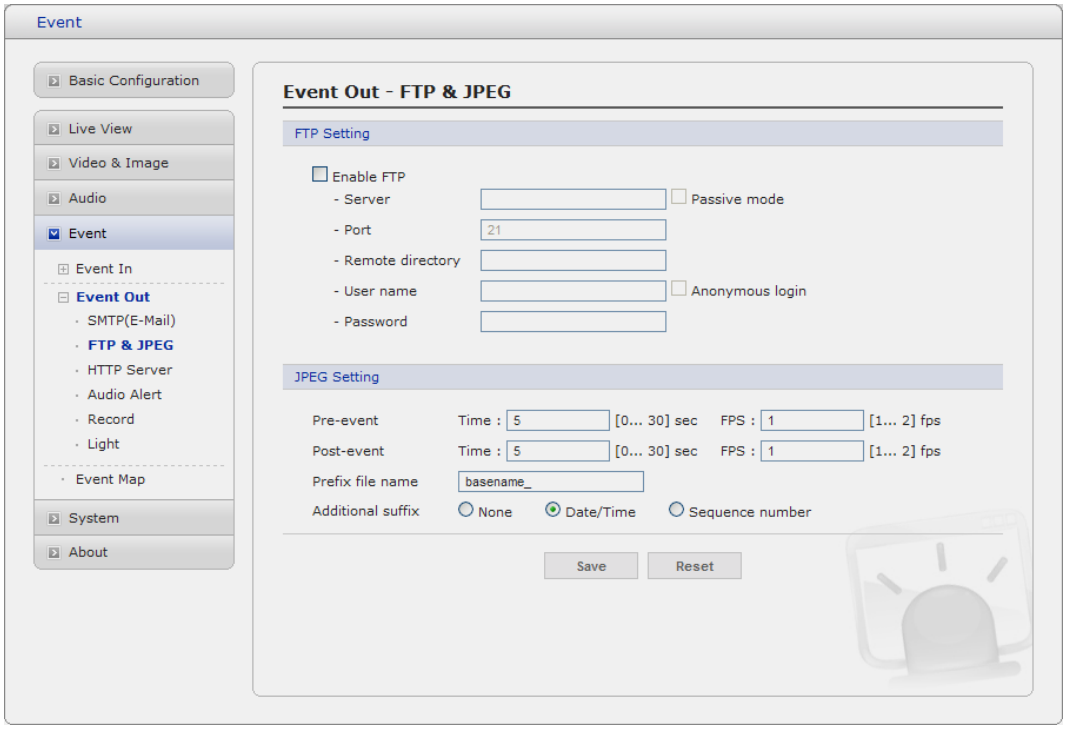
  To ensure that the login procedure is performed as securely as possible when using SMTP authentication, you must define the weakest authentication method allowed.

- **Login Method:** Set the Weakest method allowed to the highest/safest method supported by the mail server. The most secure method is listed in the drop-down list:
  Login / Plain

- **SMTP(E-Mail) Receiver**
  - **Receiver:** Enter an email address. You can also register the e-mail address of recipients up to 8.

- **SMTP(E-Mail) Test**
  - **Receiver:** Enter an email address and click the Test button to test that the mail servers are functioning and that the email address is valid.

▼ FTP & JPEG

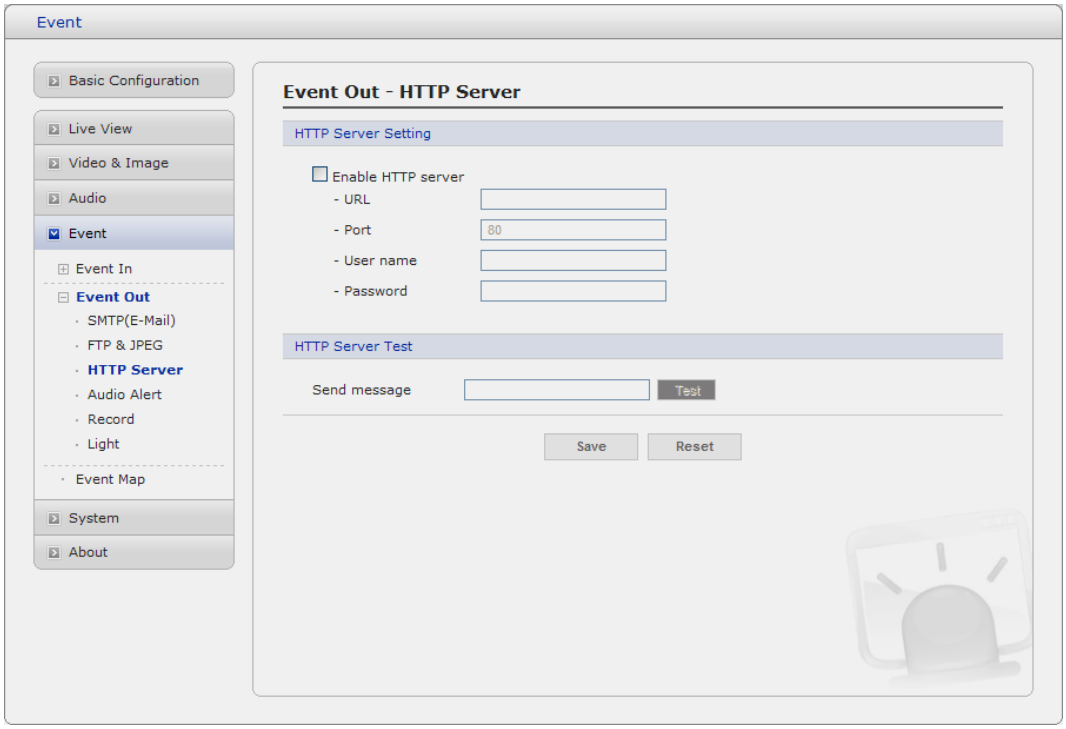


When the network camera detects an event, it can record and save images to an FTP server. Images can be sent as e-mail attachments. Check the box to enable the service.

- **FTP Setting**
  - **Server:** Enter the server's IP address or host name. Note that a DNS server must be specified in the TCP/IP network settings if using a host name.
  - **Port:** Enter the port number used by the FTP server. The default is 21.
  - **Use passive mode:** Under normal circumstances the Network Camera simply requests the target FTP server to open the data connection. Checking this box issues a PASV command to the FTP server and establishes a passive FTP connection; whereby the Network Camera actively initiates both the FTP control and data connections to the target server. This is normally desirable if there is a firewall between the camera and the target FTP server.
  - **Remote directory:** Specify the path to the directory where the uploaded images will be stored. If this directory does not already exist on the FTP server, there will be an error message when uploading.
  - **User name/Password:** Provide your log-in information.

- **JPEG Setting**
  - **Pre-event:** A pre-event buffer contains images from the time immediately preceding the event trigger. These are stored internally in the server. This buffer can be very useful when checking to see what happened to cause the event trigger.
    Check the box to enable the pre-trigger buffer, enter the desired total length in seconds, minutes or hours, and specify the required image frequency.
  - **Post-event:** This function is the counterpart to the pre-trigger buffer described above and contains images from the time immediately after the trigger. Configure as for pre-event.
  - **Prefix file name:** This name will be used for all the image files saved. If suffixes are also used, the file name will take the form <prefix>.<suffix>.<extension>
  - **Additional suffix:** Add either a date/time suffix or, a sequence number - with or without a maximum value

▼ HTTP Server

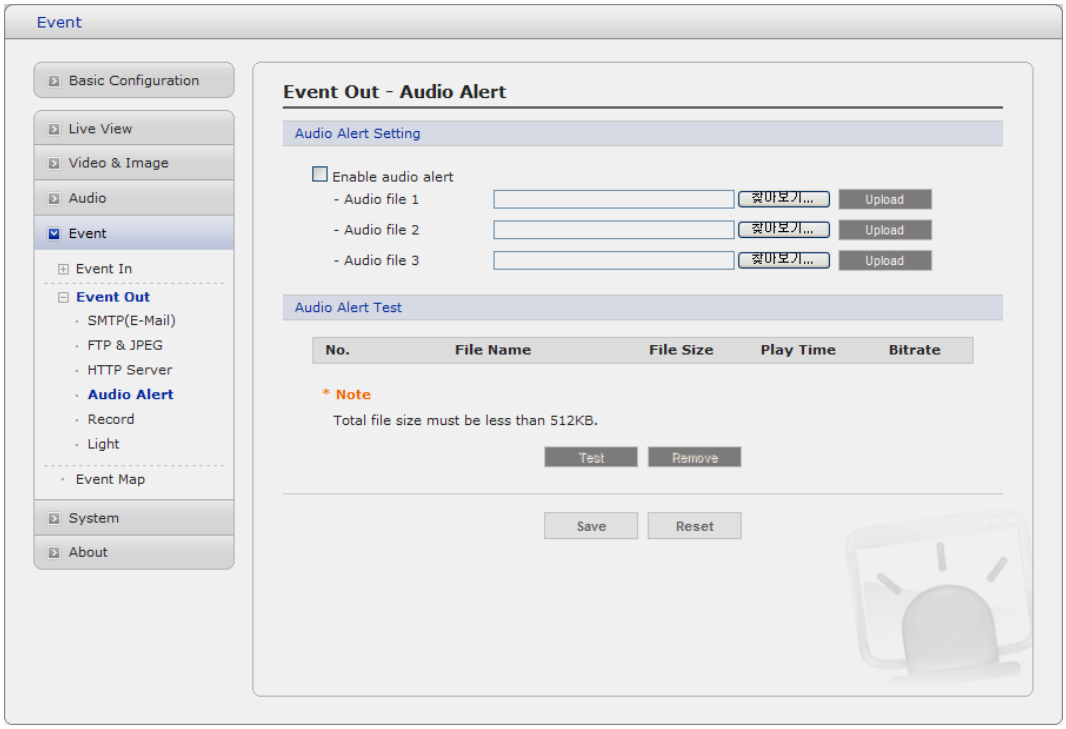


When the network camera detects an event, HTTP Server is used to receive uploaded image files and/or notification messages. Check the box to enable the service.

- **HTTP Server Setting**
  - **URL:** The network address to the server and the script that will handle the request.
    For example: http://192.168.12.244/cgi-bin/upload.cgi
  - **Port:** Enter the port number used by the HTTP server. The default is 80.
  - **User name/Password:** Provide your log-in information.

- **HTTP Server Test**
  When the setup is complete, the connection can be tested by clicking the Test button.

▼ Audio Alert



When the network camera detects an event, it can output a predefined audio data to external speaker. Check the box to enable the service.

- **Audio Alert Setting**
  To use the audio alert with the Network camera, an audio data file made by user must be uploaded from your PC. Provide the path to the file directly, or use the Browse button to locate it. Then click the Upload button.

  An audio file for Audio Alert can be made by Audio Recorder tool in the VK2-Client software.

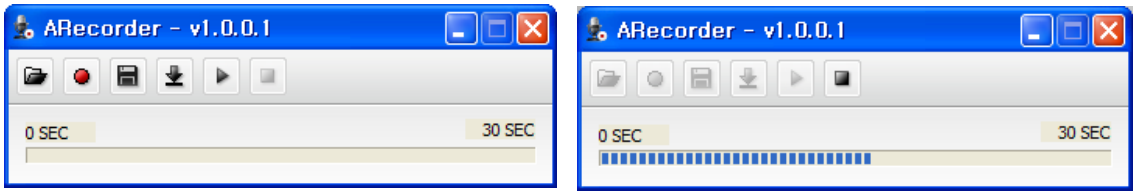
- **Audio Alert Test**
  When the setup is complete, the audio output can be tested by clicking the Test button.
  To remove an audio file, select index and click the Remove button.

Note: For a proper operation of Audio Alert, you must enable “full duplex” in Audio setting page.

Audio Recorder

To use Audio Recorder tool to make an audio file for Audio Alert function, you must install the VK2-Client on the installation CD at first.

The VK2-Client program (Start>All Programs> VK2-Client>Tools> ARecorder) in your PC, the ARecorder window will be displayed as below.



The description of each button in the ARecorder window follows.

Open: Open an audio file.

Capture: Capture audio from the microphone in your PC.

Save: Save a captured file to your PC. (PCM format)

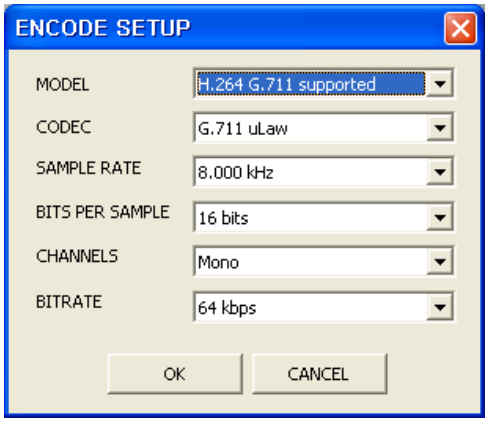
Encode: Encode a current capture file or opened PCM file to G.711 file for Audio Alert.

Play: Play a current audio file.

Stop: Stop playing audio.

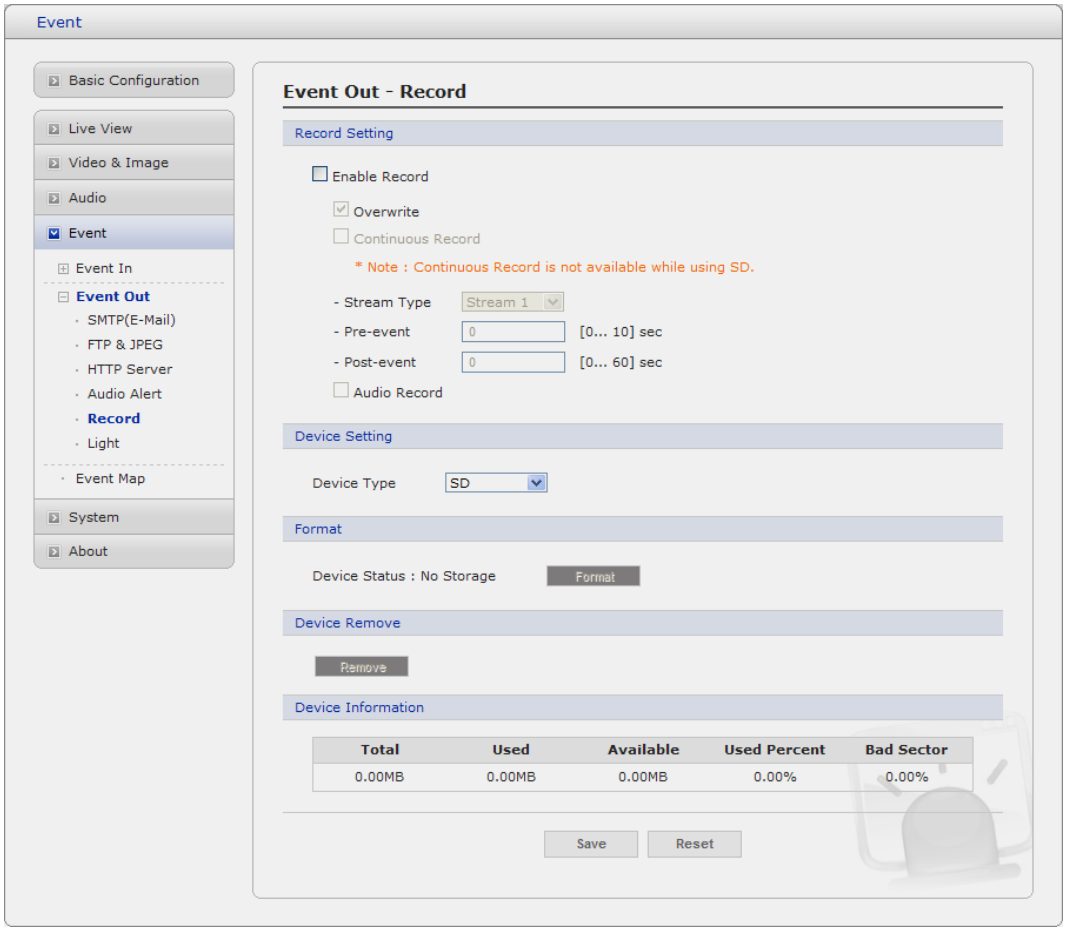
Procedures to make an audio file in G.711 format for Audio Alert.

1. Connect the microphone in your PC.
2. Click the Capture button and talk to the microphone to record the audio or voice.
   You can record up to 30 seconds. Click the Stop button to stop on capturing.
3. Click the Save button and then set the file name to save a current capture file with PCM format.
   If you don't need to make any PCM file, skip this step and then go to the step 5 directly.
4. Click the Open button and then select the file name to open an audio file in PCM format.
5. Click the Encode button to encode a current audio file to G.711 format for Audio Alert.
   Set the file name and encode parameters.



Caution: All parameters must be synchronized with ones in audio setting page of network devices for a proper operation.

▼ Record



When the network camera detects an event, it can record video stream in the Micro SD Memory (not supplied) or NAS (Network Attached Device) as a storage device. Check the box to enable the service.

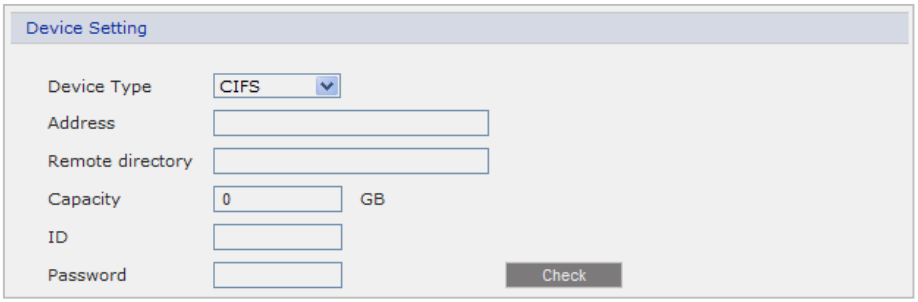
- **Record Setting**
  - **Overwrite:** Click checkbox to overwrite the storage device.
  - **Stream Type:** You can select Stream1, Stream2, or Stream3.
    * **Stream1:** H.264 or MPEG-4 data
    * **Stream2:** MJPEG data
    * **Stream3:** You can select VIDEO or IMAGE.
  - **Pre-event:** Enter pre-event time value for storage device pre-recording.
  - **Post-event:** Enter post-event time value for storage device post-recording.

- **Device Setting**

  Select Device Type to be recorded in the drop-down list.
  - **SD:** built-in SD card
  - **CIFS:** A file format for a NAS device.
  - **NFS:** A file format for a NAS device.

  Note1: Common Internet File System (CIFS) is a remote file access protocol that forms the basis for Windows file sharing, network printing, and various other network services. CIFS requires a large number of request/response transactions and its performance degrades significantly over high-latency WAN links such as the Internet.

Note2: Network File System (NFS) is a network file system protocol, allowing a user on a client computer to access files over a network in a manner similar to how local storage is accessed. NFS, like many other protocols, builds on the Open Network Computing Remote Procedure Call (ONC RPC) system.

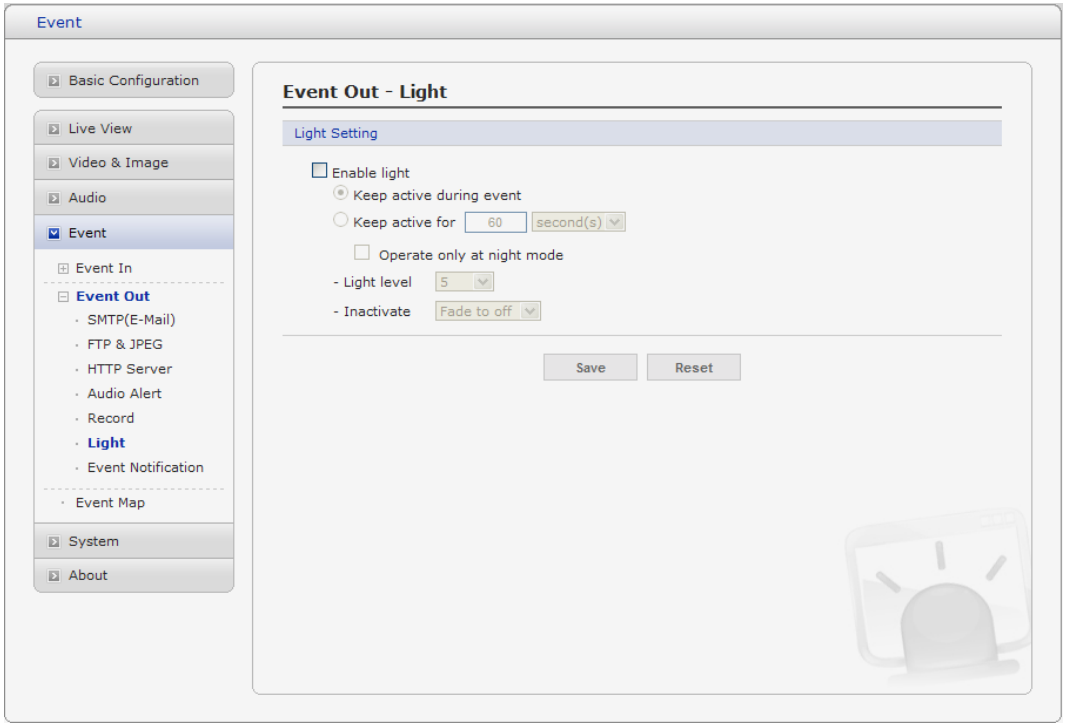


* **Address:** Enter IP address for NAS device.
* **Remote Directory:** Enter directory or folder location to be recorded in the NAS device.
* **Capacity:** Enter the capacity of storage to be used. It must be less than the total storage capacity.
* **IP/Password:** Enter ID and Password. The network camera will ask them whenever you access NAS device.
* **Check:** Press the Check button to check the validity of Device Setting data.

- **Format**
  Click the Format button to format SD card.

- **Device Information**
  Show current SD card information.

▼ **Light**

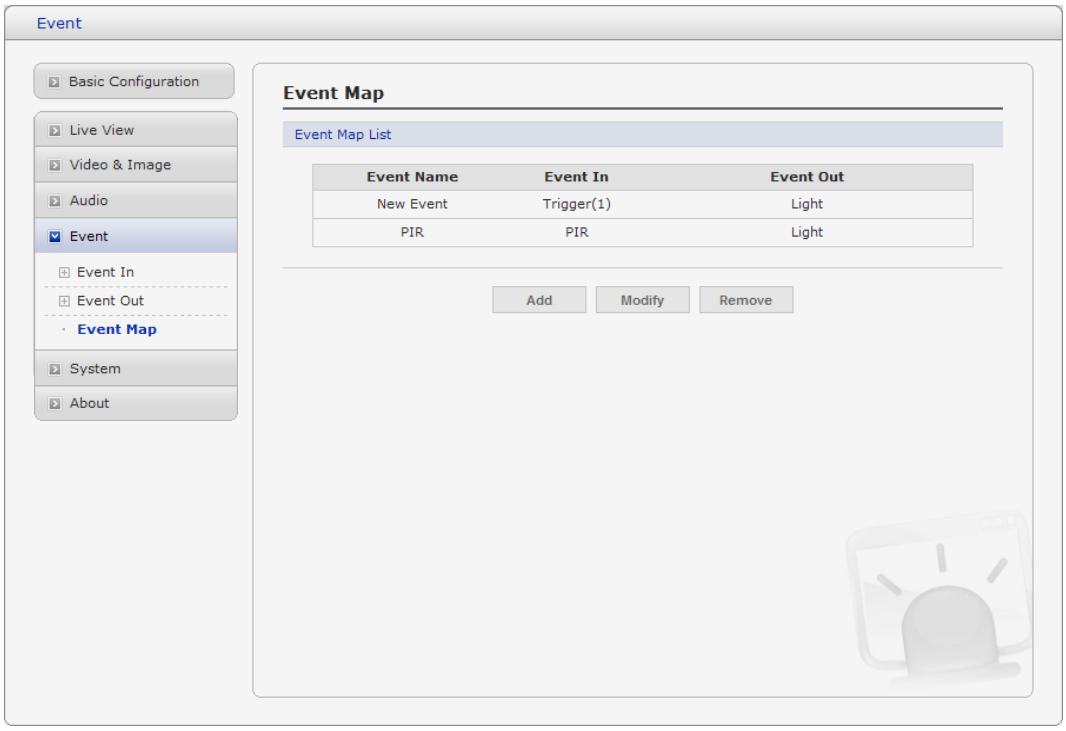


The LED on the front of the camera can be set to illuminate for a configurable interval when an event is triggered.

- **Enable light:** Select “Enable” to activate the light operation.

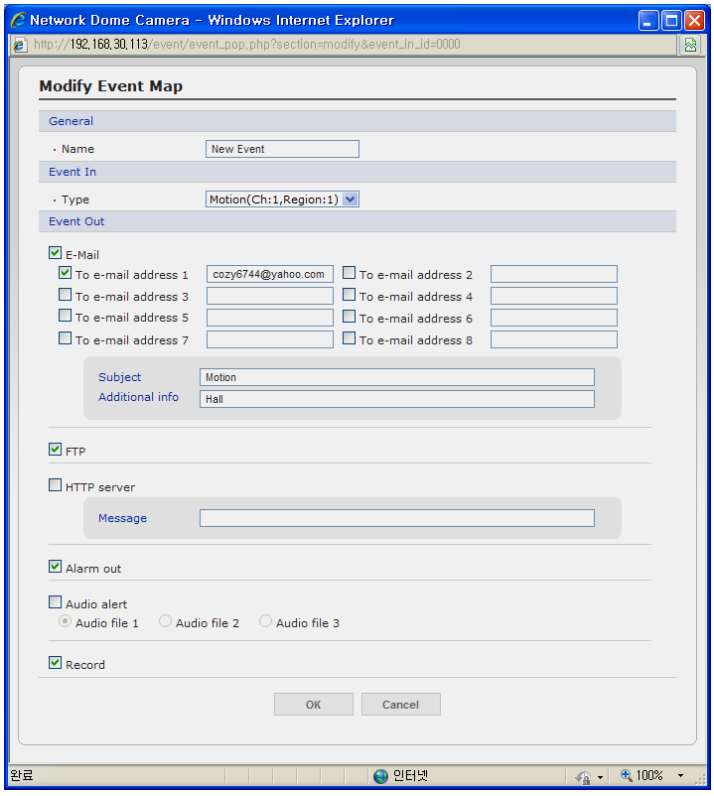
  - **Keep active during event:** Select checkbox the light keeps on during event dwell time.
  - **Keep active for:** Select checkbox the light keeps on for selected seconds or minutes.
  - **Operate only at night mode:** Selectable in the keep active for mode, the light does not operate in day time or bright ambient environment.
  - **Light level:** Be used to adjust the level of the light from 10-100%. The default level is 50%.
  - **Inactivate:** Select drop box lists between ‘fade to off’ and ‘off’

3) Event Map



The event map allows you to change the settings and establish a schedule for each event trigger from the Network Camera. You can register the event map up to max. 15.

Click Add button to make a new event map and you can see a popup window as below.



- **General**
  Enter the name for a new event map.

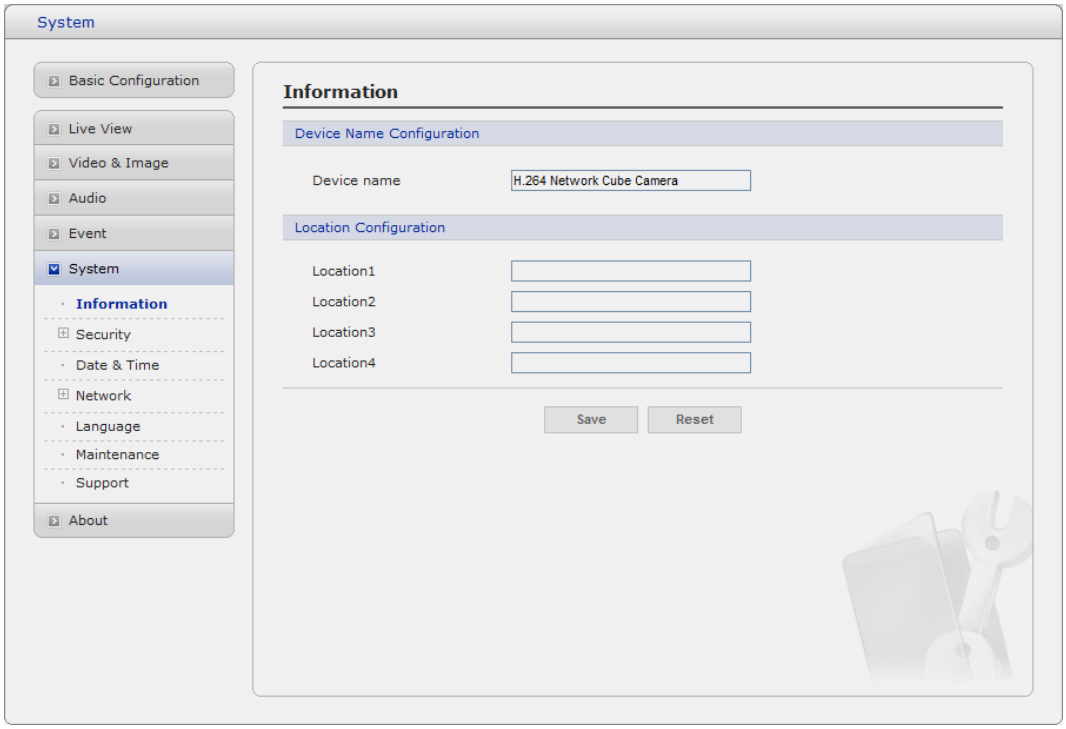
- **Event In**
  Select an event type in the drop down list.

- **Event Out**
  - **E-mail:** Select email addresses you want to send via email that an event has occurred.
  - **FTP:** Select checkbox beside FTP to record and saves images to an FTP server when an event has occurred.
  - **HTTP Server:** It sends notification messages to an HTTP server that listens for these. The destination server must first be configured on the Event In page. Enter a message you want to send.
  - **Audio Alert:** Select a Audio alert file the Network Camera output when audio alert event triggered. The Audio alert file must first be configured on the Event In page.

3.5.5 System

1) Information

You can enter the system information. This page is very useful when you refer device information after installation.

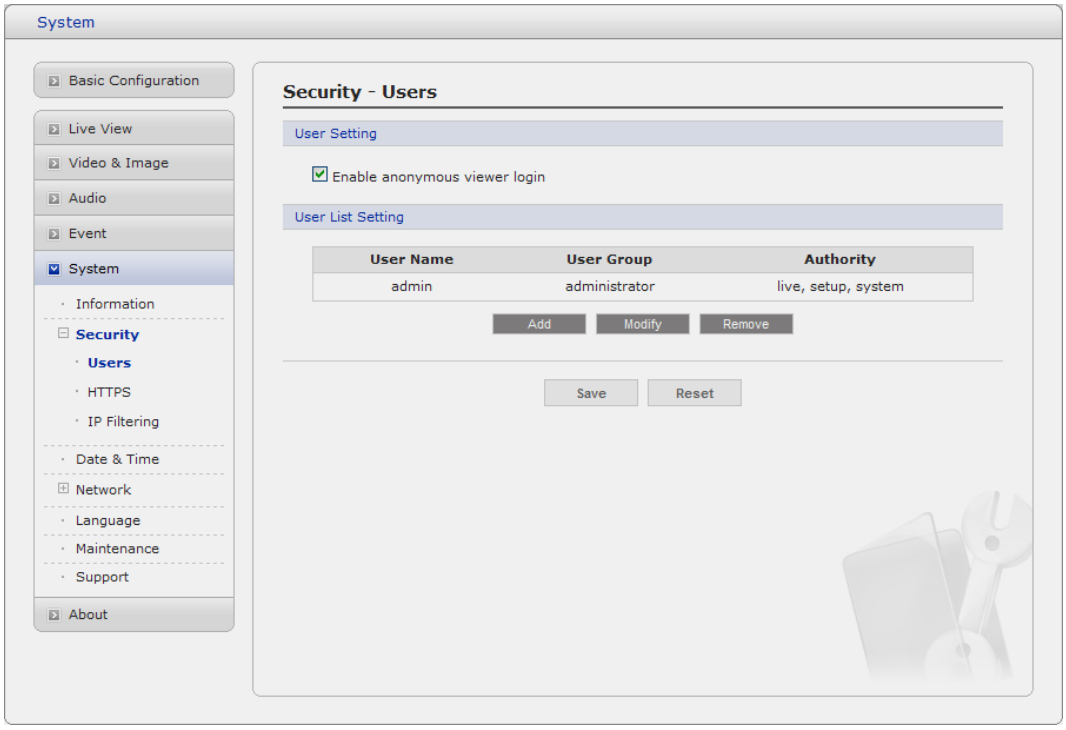


- **Device Name Configuration**
  Enter the device name.

- **Location Configuration**
  Enter the location information. You can enter that by four.

2) Security

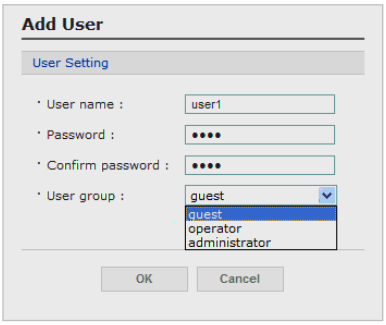
▼ Users



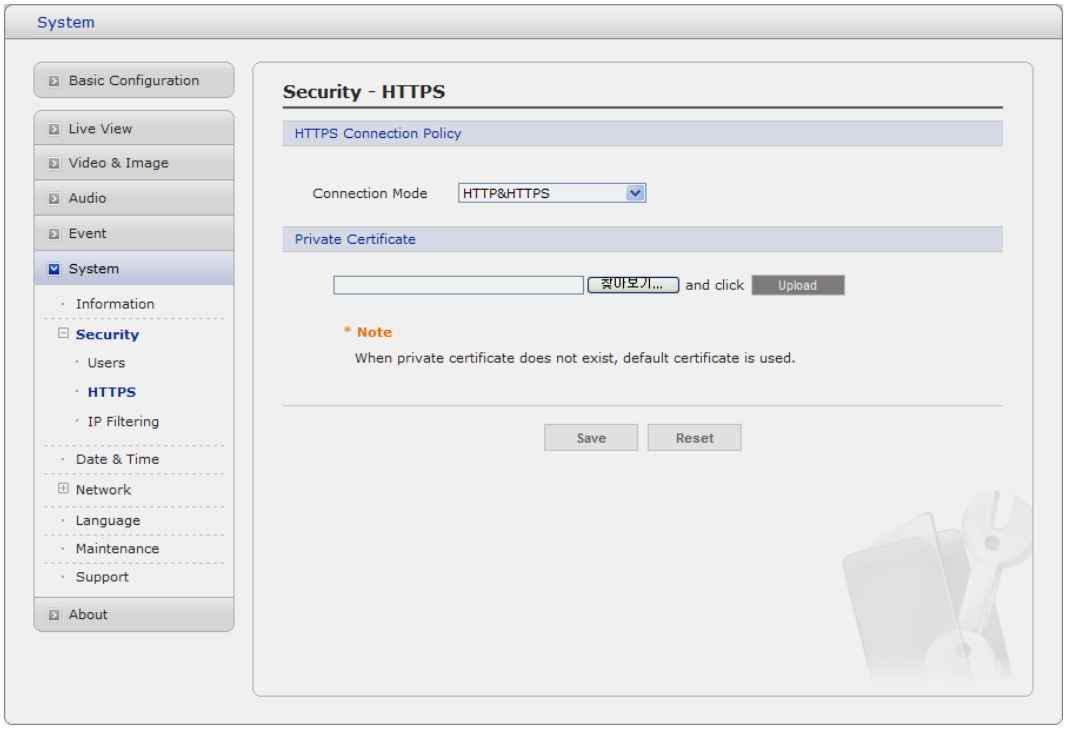
User access control is enabled by default, when the administrator sets the root password on first access. New users are authorized with user names and passwords, or the administrator can choose to allow anonymous viewer login to the Live View page, as described below:

- **User Setting**
  Check the box to enable anonymous viewer login to the Network Camera without the user account. When using the user account, users have to try log-in at every access.

- **User List Setting**
  This section shows a registered user account. Enter a user name and password to be added, and register them by pressing the Add button. You can see the pop-up window as below.



▼ **HTTPS**



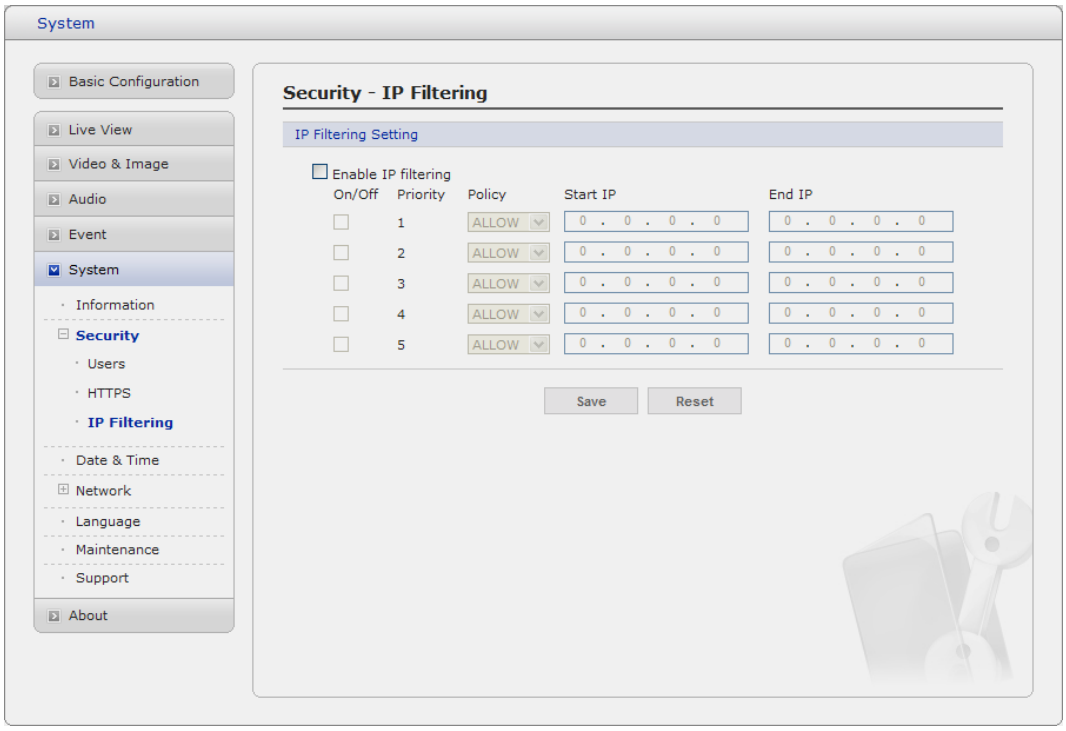
For greater security, the Network Camera can be configured to use HTTPS (Hypertext Transfer Protocol over SSL (Secure Socket Layer)). That is, all communication that would otherwise go via HTTP will instead go via an encrypted HTTPS connection.

- **HTTPS Connection Policy**
  Choose the form of connection you wish to use from the drop-down list for the administrator, Operator and Viewer to enable HTTPS connection (set to HTTP by default).
  - HTTP
  - HTTPS
  - HTTP & HTTPS

- **Upload Certificate**
  To use HTTPS for communication with the Network Camera, An official certificate issued by a CA (Certificate Authority) must be uploaded from your PC. Provide the path to the certificate directly, or use the **Browse** button to locate it. Then click the **Upload** button.

Please refer to the home page of your preferred CA for information on where to send the request. For more information, please see the online help.

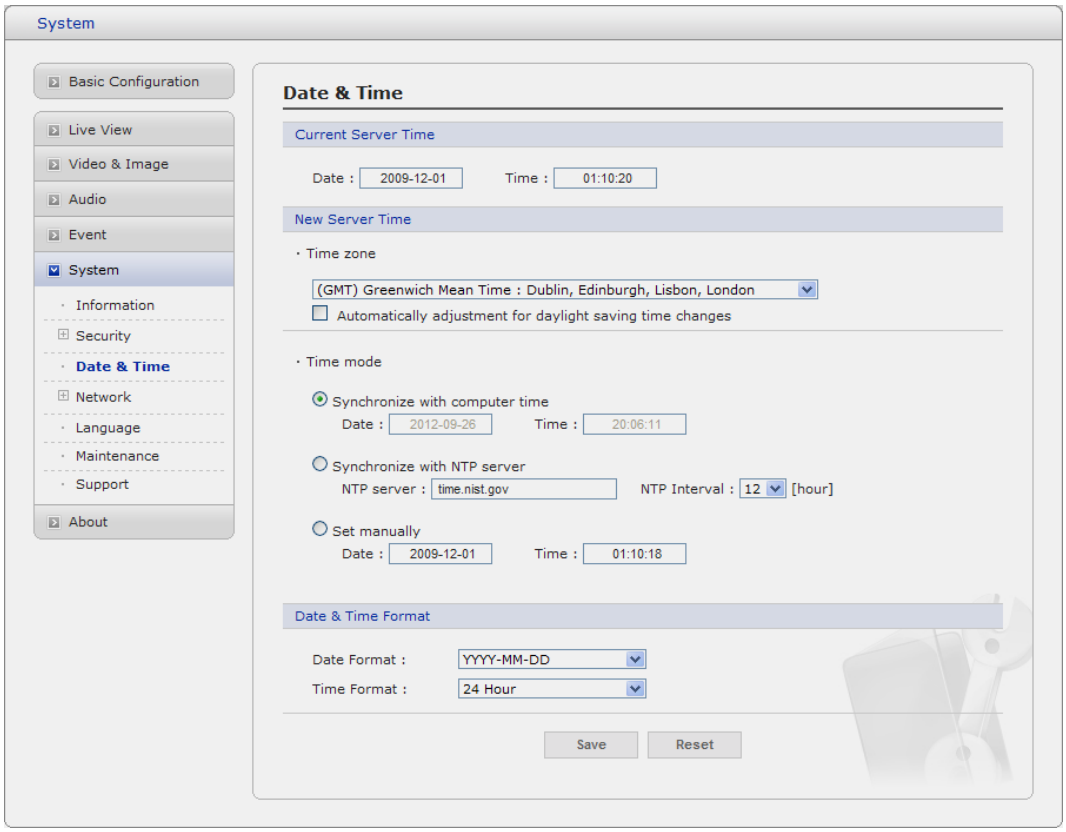
▼ IP Filtering



Checking the **Enable IP address filtering** box enables the IP address filtering function. Up to 256 IP address entries may be specified (a single entry can contain multiple IP addresses). Click the **Add** button to add new filtered addresses.
When the IP address filter is enabled, addresses added to the list are set as allowed **or** denied addresses. All other IP addresses not in this list will then be allowed or denied access accordingly, that is, if the addresses in the list are allowed, then all others are denied access, and vice versa. See also the online help for more information.

Note that users from IP addresses that will be allowed must also be registered with the appropriate access rights (Guest, Operator or Administrator). This is done from Setup> System>Security>Users.

3) Date & Time



- **Current Server Time**
  It displays the current date and time (24h clock). The time can be displayed in 12h clock format in the overlay (see below).

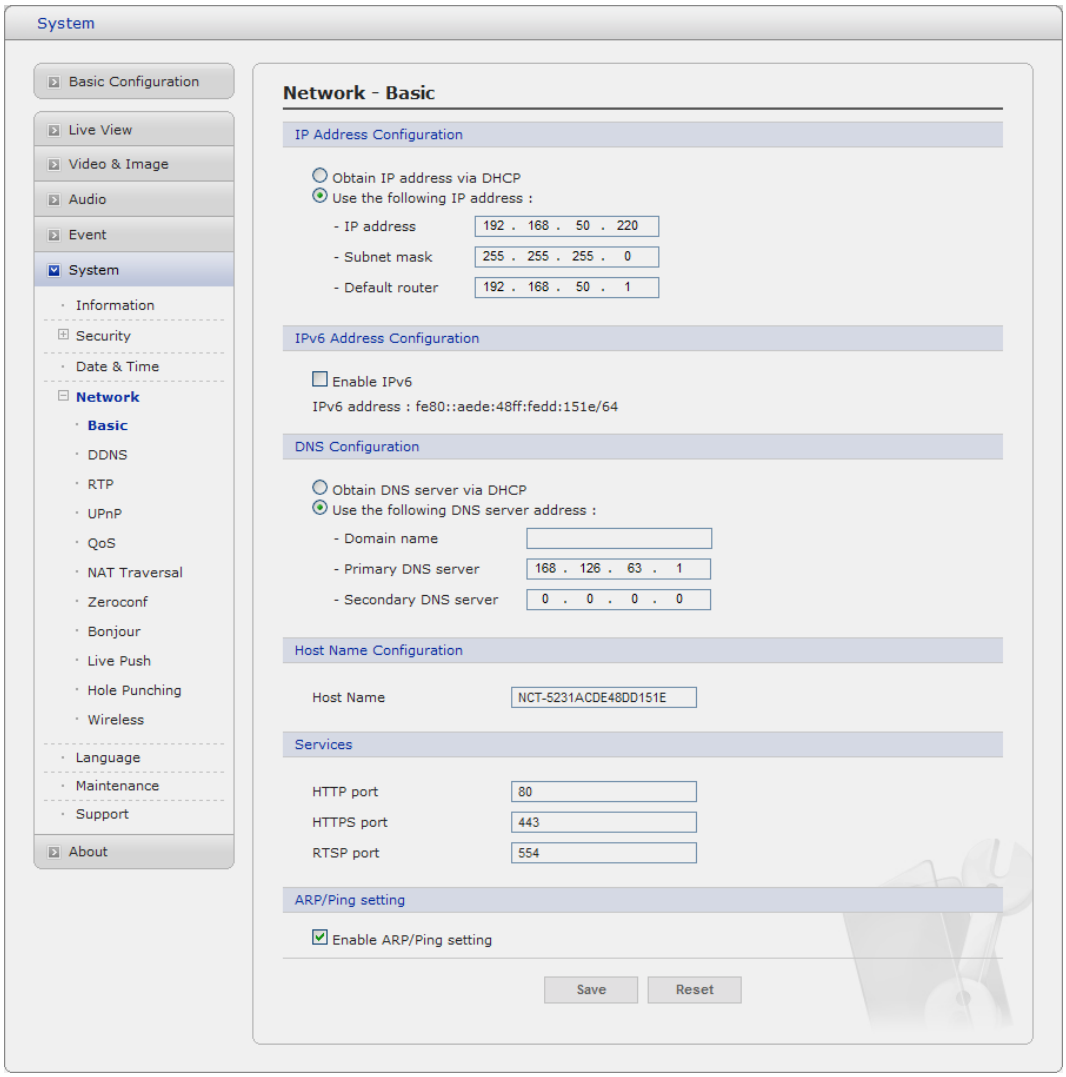
- **New Server Time**
  Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, select “Automatically adjustment for daylight saving time changes”.

  From the Time Mode section, select the preferred method to use for setting the time:
  - **Synchronize with computer time:** sets the time from the clock on your computer.
  - **Synchronize with NTP Server:** the network camera will obtain the time from an NTP server every 60 minutes.
  - **Set manually:** this option allows you to manually set the time and date.

- **Date & Time Format**
  Specify the formats for the date and time (12h or 24h) displayed in the video streams.
  Select Date & Time format from the drop-down list.
  - **Date Format:** Specify the date format. YYYY: Year, MM: Month, DD: Day
  - **Time Format:** Specify the date format. 24Hours or 12 Hours

Note: Note that if using a host name for the NTP server, a DNS server must be configured under TCP/IP settings.

4) Network



Setting in regard to network can be executed. Settings for IP, DNS, Host Name, Port, and ARP/Ping can be established, along with setting for DDNS, uPnP, QoS, Zeroconfig, Bonjour, Live Push, Hole Punching, and wireless.

▼ **Basic**

- **IP Address Configuration:**
  - **Obtain IP address via DHCP:** Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address.
  - **Use the following IP address:** To use a static IP address for the Network Camera, check the radio button and then make the following settings:
  * **IP address:** Specify a unique IP address for your Network Camera.
  * **Subnet mask:** Specify the mask for the subnet the Network Camera is located on.
  * **Default router:** Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

- **IPv6 Address Configuration**
  Check this box to enable IPv6. Other settings for IPv6 are configured in the network router.

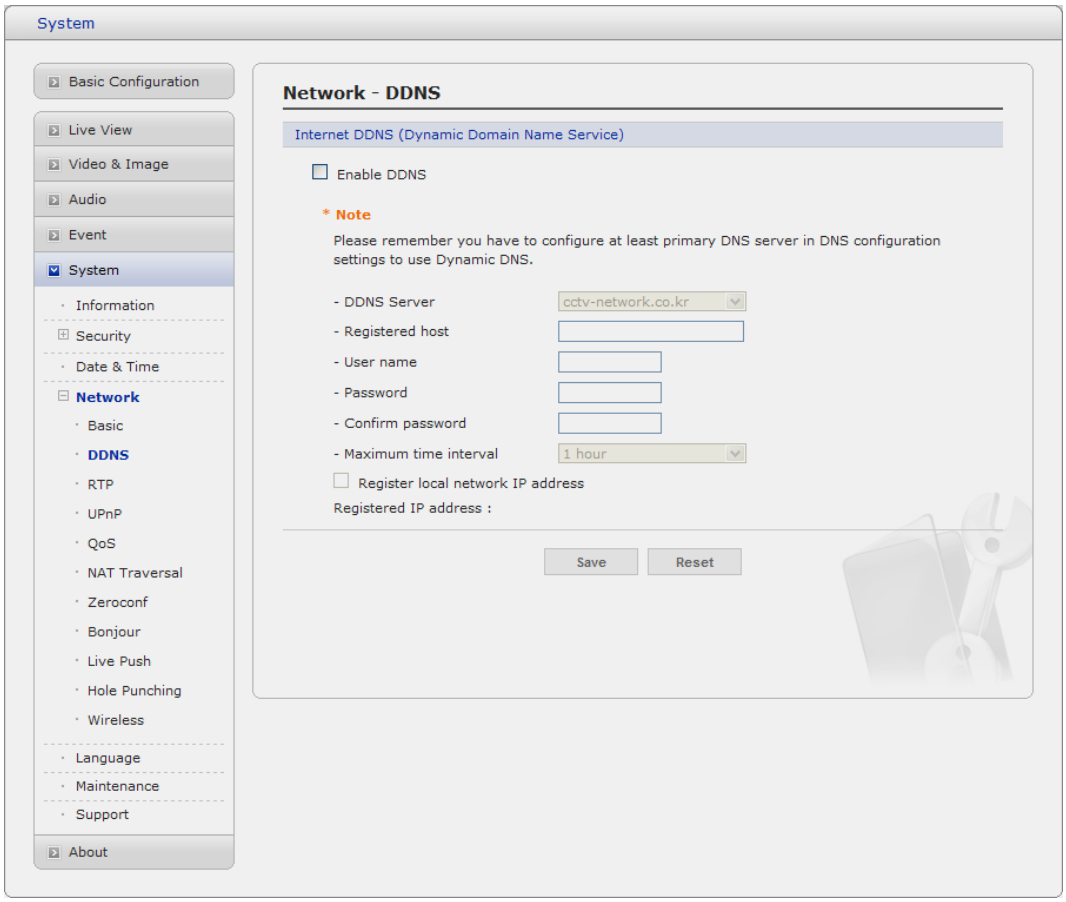
- **DNS Configuration**
  DNS (Domain Name Service) provides the translation of host names to IP addresses on your network.
  - **Obtain DNS Server via DHCP:** Automatically use the DNS server settings provided by the DHCP server.
  - **Use the following DNS server address**: enter the desired DNS server by specifying the following:
  * **Domain name:** enter the domain(s) to search for the host name used by the Network Camera. Multiple domains can be separated by semicolons (;). The host name is always the first part of a Fully Qualified Domain Name, for example, myserver is the host name in the Fully Qualified Domain Name myserver.mycompany.com where mycompany.com is the Domain name.
  * **DNS servers:** enter the IP addresses of the primary and secondary DNS servers.

- **Host Name Configuration**
  - **Host Name:** enter the host name to be used as device information in the client software or SmartManager.

- **Services**
  - **HTTP port:** Enter a port to receive a service through the HTTP. Default Port Number is '80'.
  - **HTTPS port:** Enter a port to receive a service through the HTTPS. Default Port Number is '443'.
  - **RTSP port:** Enter a port to receive a service through the RTSP. Default Port Number is '554'.

- **ARP/Ping Setting**
  - Enable ARP/Ping setting of IP address - The IP address can be set using the ARP/Ping method, which associates the unit's MAC address with an IP address. Check this box to enable the service.
    Leave disabled to prevent unintentional resetting of the IP address.

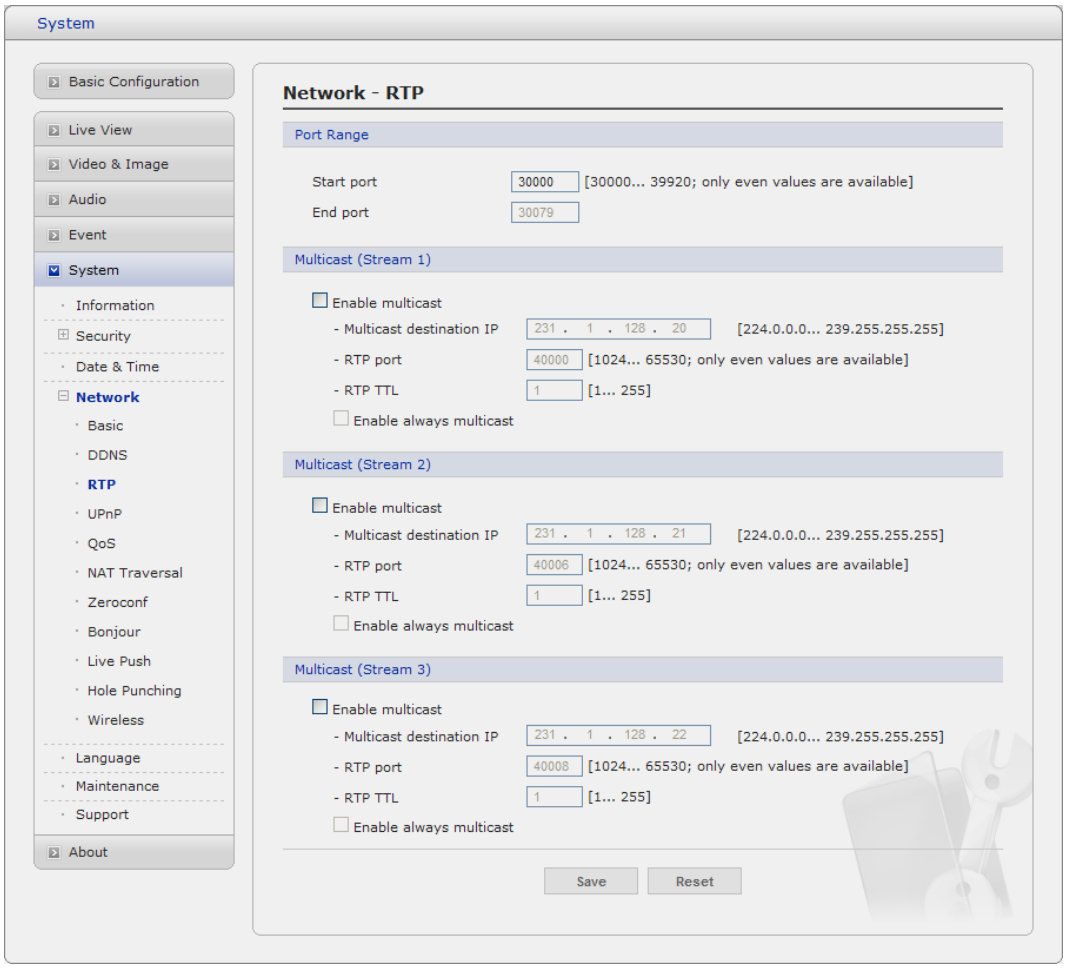
▼ **DDNS**



- **Internet DDNS(Dynamic Domain Name Service)**
  When using the high-speed Internet with the telephone or cable network, users can operate the Network Camera even on the floating IP environment in which IPs are changed at every access. Users should receive an account and password by visiting a DDNS service like http://www.dyndns.com/, or http://www.cctv-network.co.kr/.

  - **Enable DDNS:** Check to get DDNS service to be available.
    * **DDNS Server:** Select the DDNS server.
    * **Registered host:** Enter an address of the DDNS server.
    * **Username:** Enter an ID to access to the DDNS server.
    * **Password:** Enter a password to be used for accessing the DDNS server.
    * **Confirm:** Enter a password again to confirm it.
    * **Maximum time interval:** Set a time interval to synchronize with the DDNS server. Select an item in the interval drop-down list.
    * **Register local network IP address:** Register a Network Video Server IP address to the DDNS server

▼ **RTP**

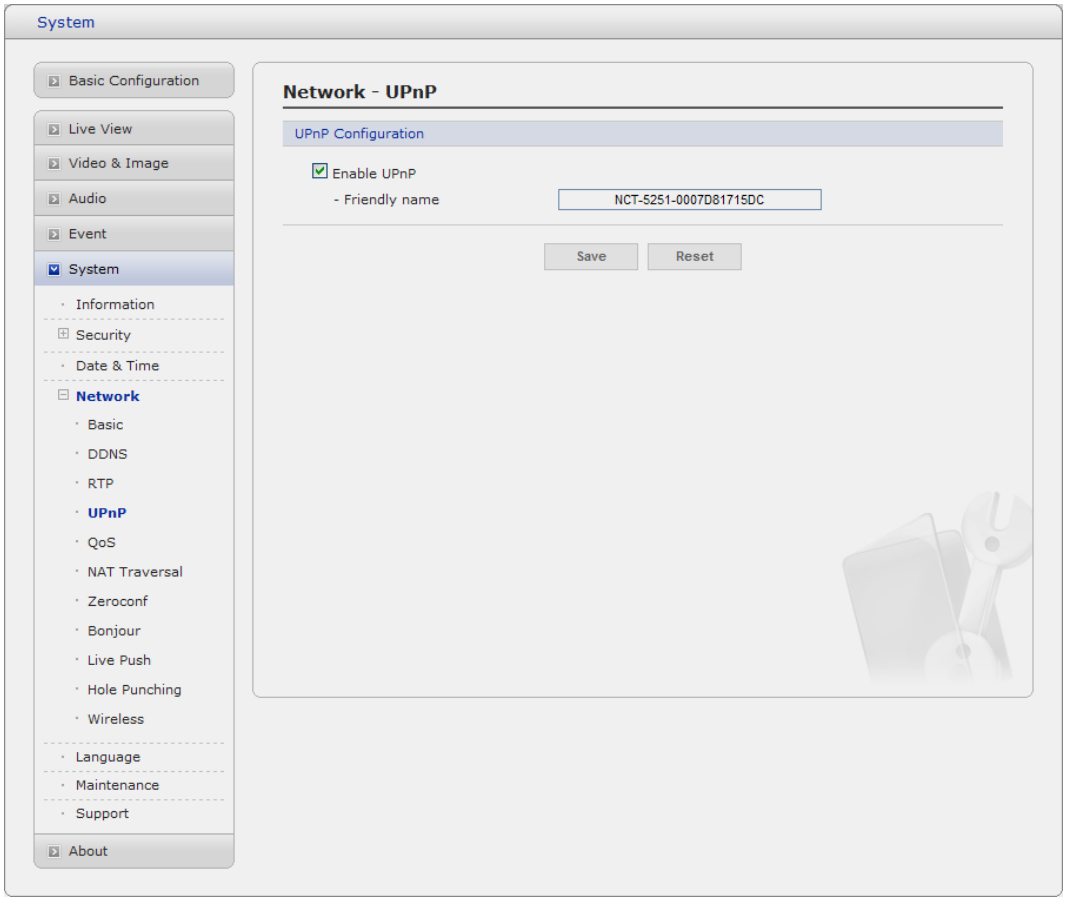


Have a setting for sending and receiving an audio or video on a real-time basis. These settings are the IP address, port number, and Time-To-Live value to use for the media stream(s) in multicast H.264 format. Only certain IP addresses and port numbers should be used for multicast streams. For more information, please see the online help.

- **Port Range**
  - **Start port:** Enter a value between 1024 and 65532

- **Multicast**
  This function is for sending Video and Audio to Multicast group.
  - **Enable Multicast:** Check the checkbox to enable multicast operation.
  - **Multicast destination IP:** Enter an IP between 224.0.0.0 and 239.255.255.255.
  - **RTP port:** Enter a value between 1024 and 65532.
  - **RTP TTL:** Enter a value between 1 and 255. If a network status is smooth, enter a lower value. On the other hand, if a network status is poor, enter a higher value. When there are many Network Cameras or users, a higher value may cause a heavy load to the network. For a detailed setting, please consult with a network manager.

▼ **UPnP**



The Network Camera includes support for UPnP™. UPnP™ is enabled by default, and the Network Camera then is automatically detected by operating systems and clients that support this protocol.

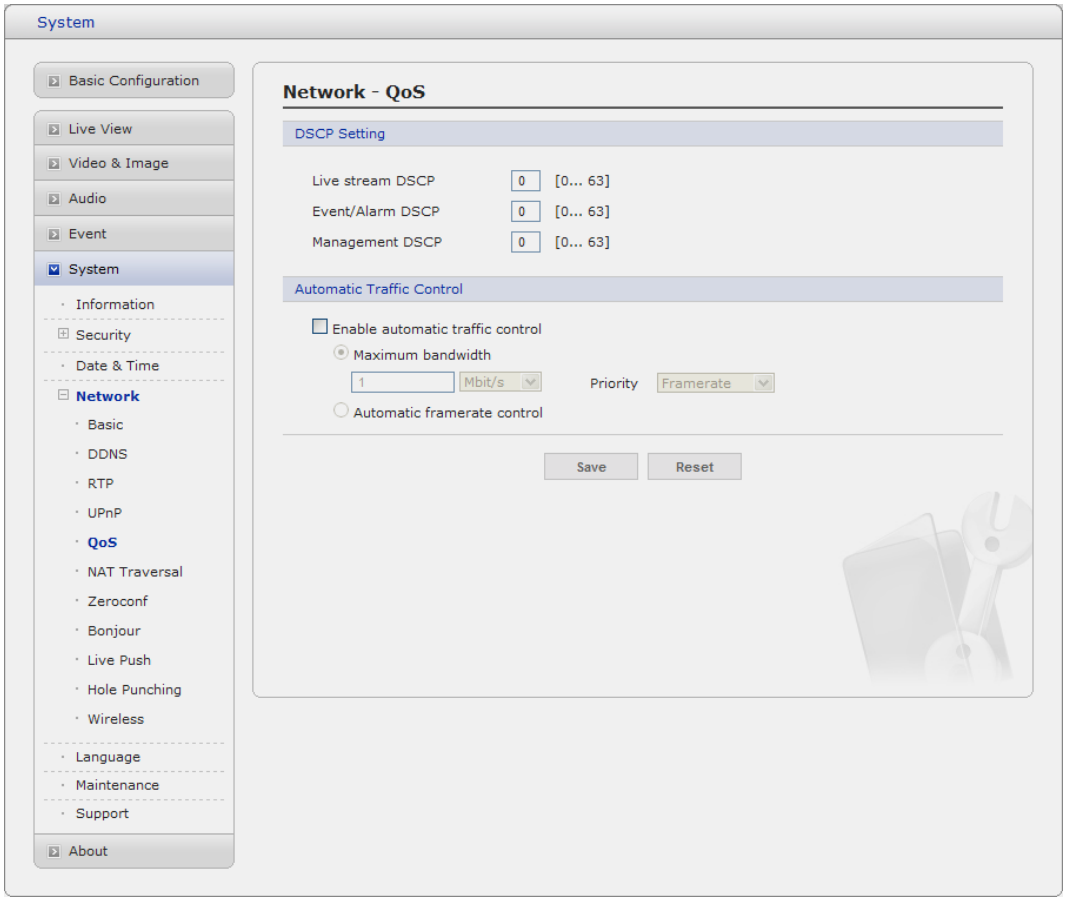
Note: UPnP™ must be installed on your workstation if running Windows XP. To do this, open the Control Panel from the Start Menu and select Add/Remove Programs. Select Add/Remove Windows Components and open the Networking Services section. Click Details and then select UPnP™ as the service to add.

▼ QoS

Quality of Service (QoS) provides the means to guarantee a certain level of a specified resource to selected traffic on a network. Quality can be defined as a maintained level of bandwidth, low latency, and no packet losses.

The main benefits of a QoS-aware network are:

- The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
- Greater reliability in the network, thanks to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications.



- **DSCP Settings**
  For each type of network traffic supported by your network video product, enter a DSCP (Differentiated Services Code Point) value. This value is used to mark the traffic's IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tell the router or switch which type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Note that DSCP values can be entered in decimal or hex form, but saved values are always shown in decimal.

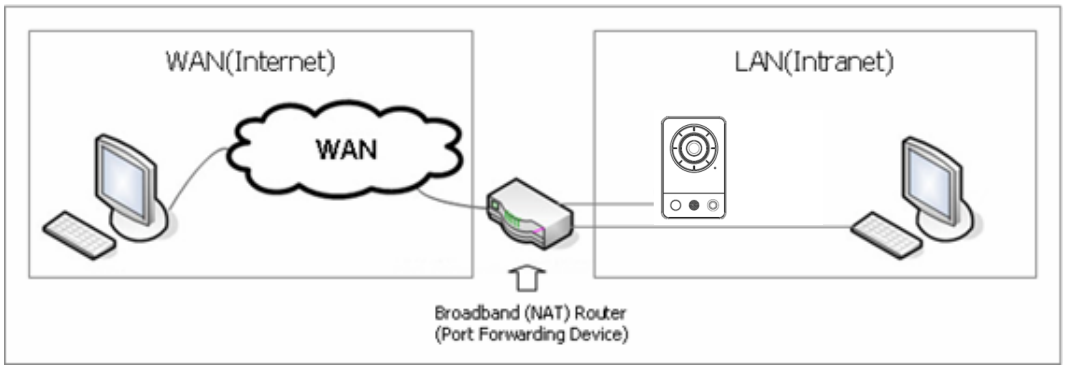
  The following types of traffic are marked:
  - **Live Stream DSCP:**
  - **Event/Alarm DSCP:**
  - **Management DSCP:**

- **Auto Traffic Control**
  Set a limitation on user network resources by designating the maximum bandwidth.
  - **Maximum bandwidth:** In case of sharing other network programs or equipment, it is possible to set a limitation on the maximum bandwidth in the unit of Mbit/s or kbit/s.
  - **Auto frame rate:** Selected if not influenced by a network-related program or equipment without a limitation on the network bandwidth.

▼ NAT Traversal

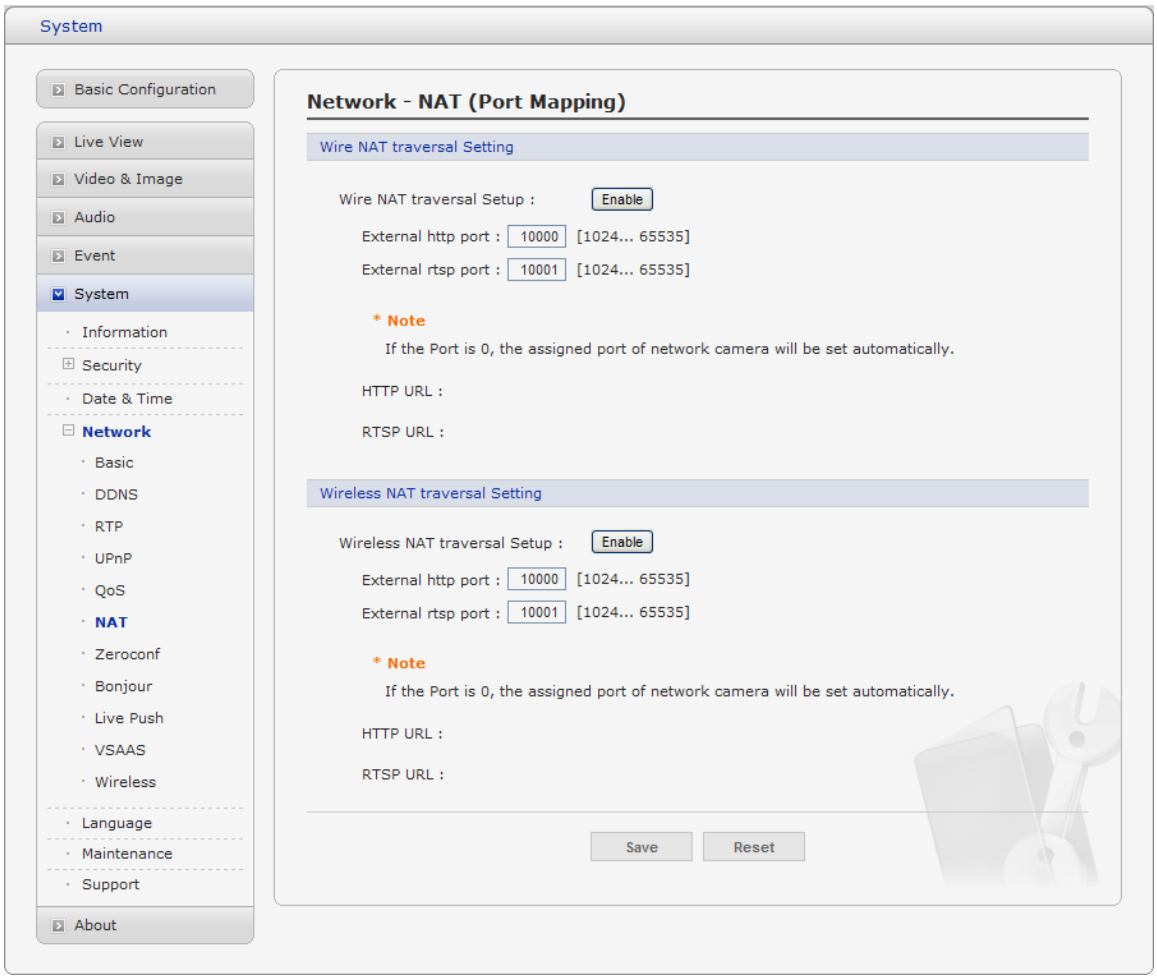
A broadband router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the “outside”, that is, the Internet. Security on the private network (LAN) is increased since most broadband routers are pre-configured to stop attempts to access the private network (LAN) from the public network/Internet.

Use **NAT traversal** when your network cameras are located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the network camera.



Notes:

- For NAT traversal to work, this must be supported by the broadband router.
- The broadband router has many different names:
  “NAT router”, “Network router“, Internet Gateway”, “Broadband sharing device” or “Home firewall” but the essential purpose of the device is the same.



- **NAT traversal Settings**

  Wire/Wireless NAT traversal setup

  - **Enable:** when enabled, the network camera attempt to configure port mapping in a NAT router on your network, using UPnP™. Note that UPnP™ must be enabled in the Network Camera (see System>Network>UPnP).

  * **External HTTP port:** Enter the external HTTP port number.

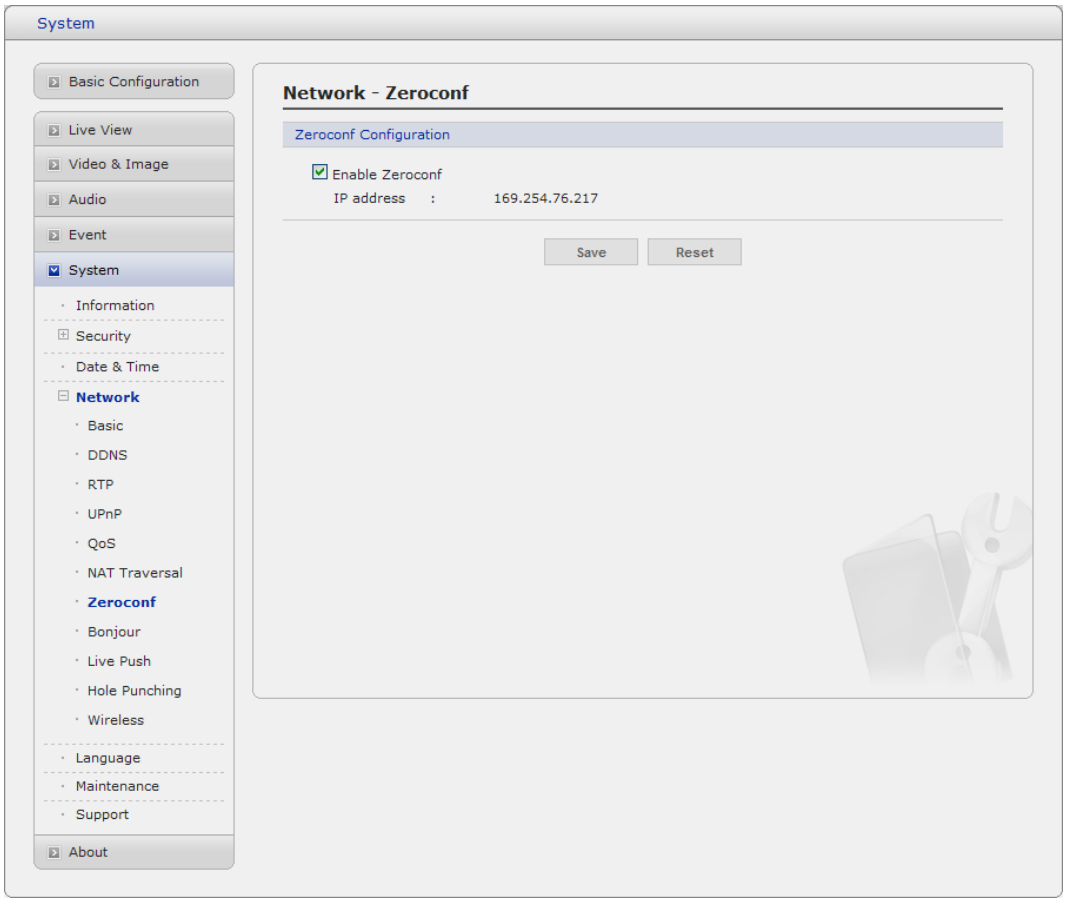
  * **External RTSP port:** Enter the external RTSP port number.

Notes:

- If you attempt to enter a port that is already in use, an alert message will be displayed.
- IGD(Internet Gateway Device) and NAT functions are necessary. Check your AP specs.

▼ Zeroconfig

Zeroconfig allows the network camera to create and assign IP address for network cameras and connect to a network automatically.



Zero configuration networking (zeroconf), is a set of techniques that automatically creates a usable Internet Protocol (IP) network without manual operator intervention or special configuration servers.

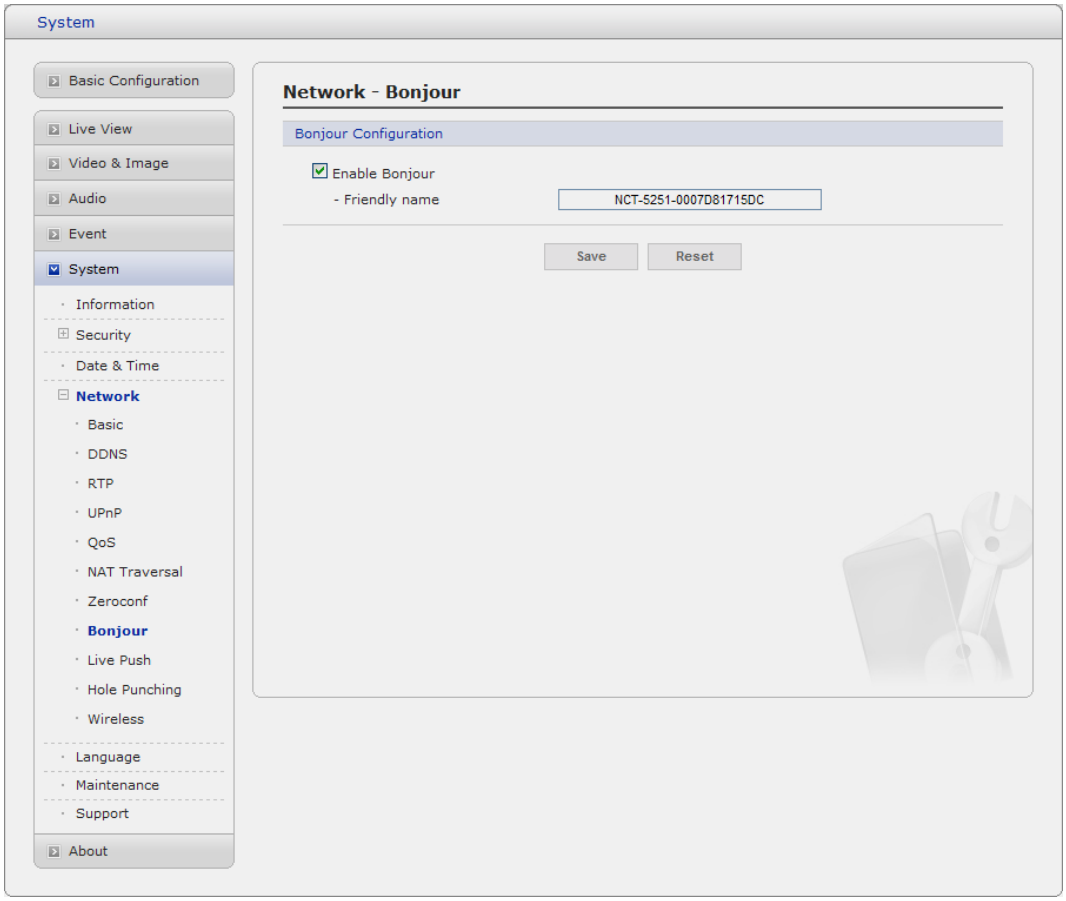
Zero configuration networking allows devices such as computers and printers to connect to a network automatically. Without zeroconf, a network administrator must set up services, such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS), or configure each computer's network settings manually, which may be difficult and time-consuming.

Zeroconf is built on three core technologies:

- Assignment of numeric network addresses for networked devices (link-local address auto configuration)
- Automatic resolution and distribution of computer hostnames (multicast DNS)
- Automatic location of network services, such as printing devices through DNS service discovery.

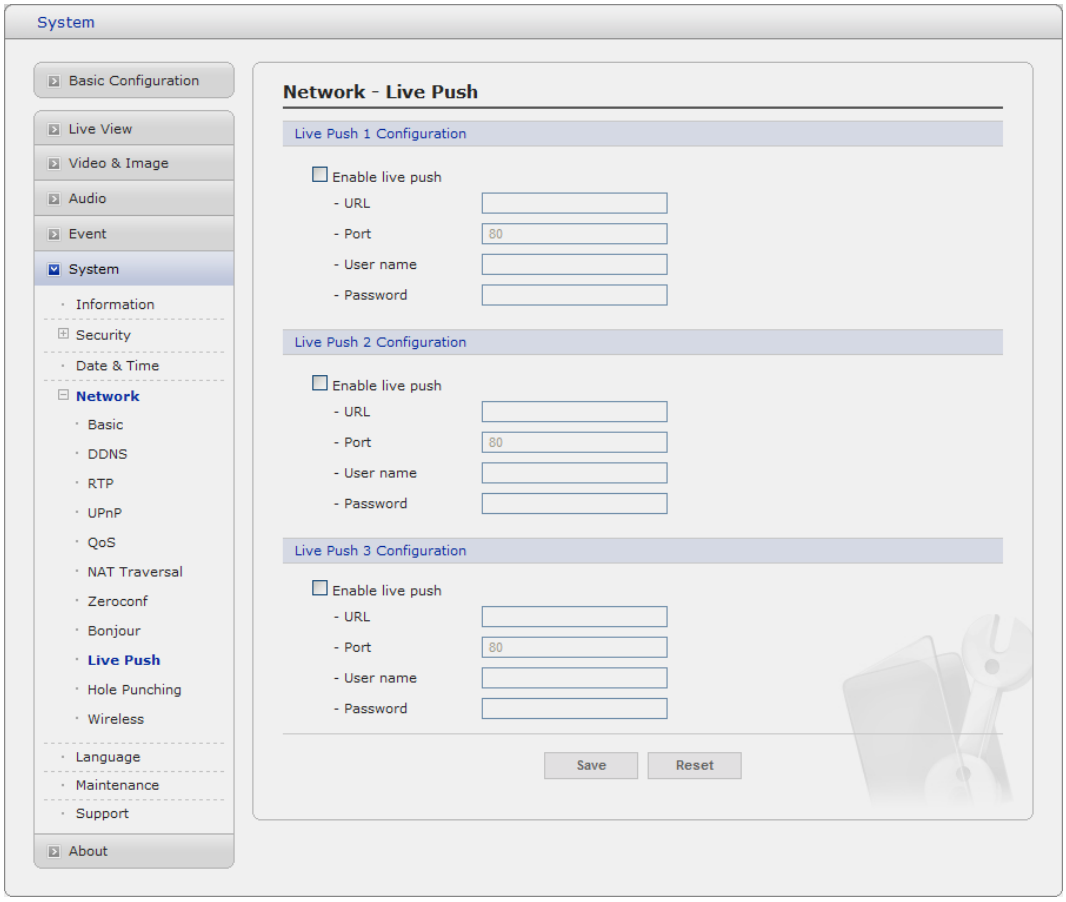
▼ Bonjour

The network camera includes support for Bonjour. When enabled, the network camera is automatically detected by operating systems and clients that support this protocol.



Note: Bonjour - Also known as zero-configuration networking, Bonjour enables devices to automatically discover each other on a network, without having to enter IP addresses or configure DNS servers. Bonjour is a trademark of Apple Computer, Inc.

▼ **Live Push**



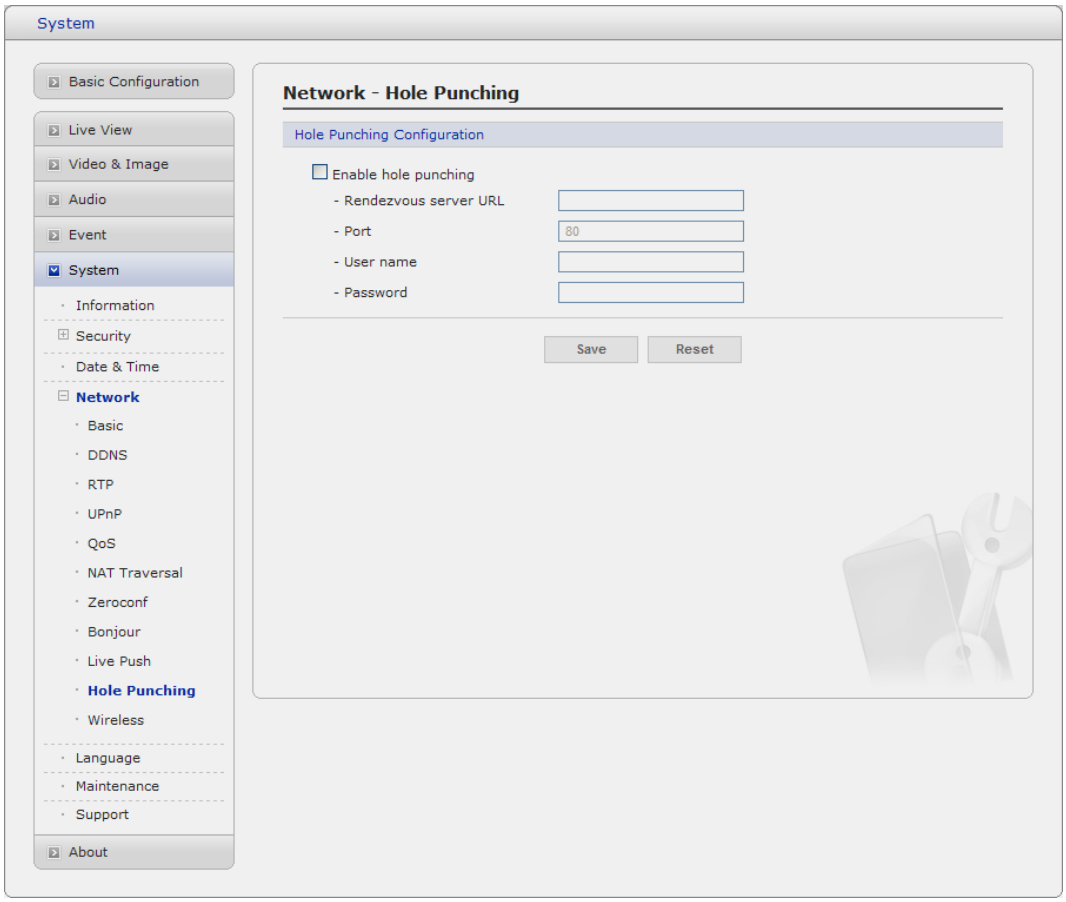
- **Live Push Configuration**

When you activate this function, the network camera as a client can transfer audio, video and event data to the registered server. The network camera and server use RTP/RTSP as the protocol for the actual transport of audio/video data.

Up to 3 servers can be configured.

- **URL:** The network address to the server and the script that will handle the request.
- **User name/Password:** Provide your log-in information. The network camera will ask them whenever you access the Live Push Server.

▼ **Hole Punching**



- **Hole Punching Configuration**

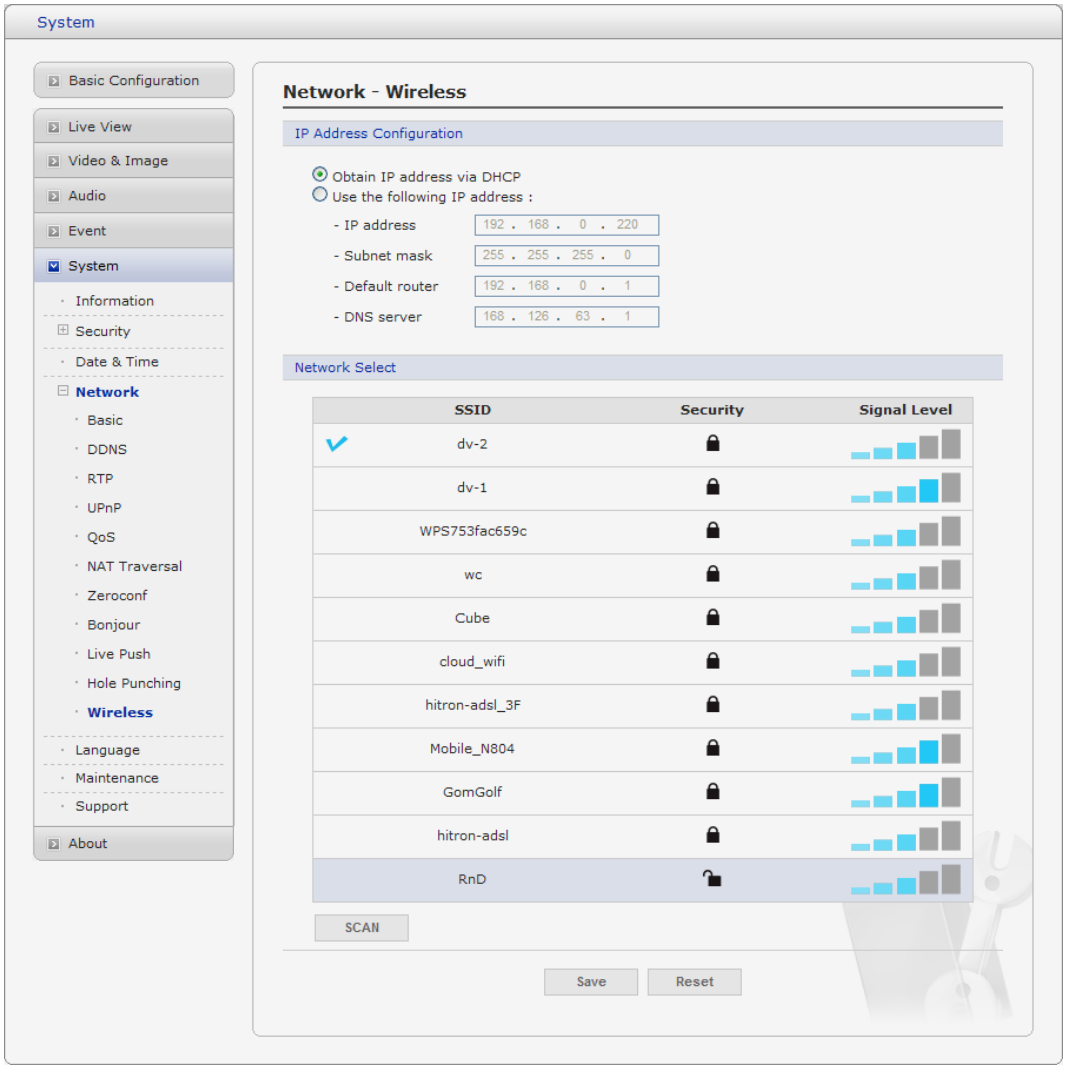
  - **Rendezvous Server URL:** Enter the third-party server's URL that uncovers external and internal address information.
  - **ID/Password:** Enter ID and Password. The network camera will ask them whenever you access the Rendezvous Server.

Note:
Hole punching is a computer networking technique for establishing communications between two parties in separate organizations who are both behind restrictive firewalls. Used for applications such as online gaming, P2P and VoIP, both clients establish a connection with an unrestricted third-party server that uncovers external and internal address information for them. Since each client initiated the request to the server, the server knows their IP addresses and port numbers assigned for that session, which it shares one to the other. Having valid port numbers causes the firewalls to accept the incoming packets from each side.

UDP hole punching is a commonly used technique employed in network address translator (NAT) applications for maintaining User Datagram Protocol (UDP) packet streams that traverse the NAT. NAT traversal techniques are typically required for client-to-client networking applications on the Internet involving hosts connected in private networks, especially in peer-to-peer and Voice over Internet Protocol (VoIP) deployments.

▼ Wireless(VK2-2MPCCW only)

Wireless settings in the VK2-2MPCCW must be the same as the access point or ad-hoc device. When changing the settings, they should always be made first in the camera and then in the wireless access point. This ensures that the camera is always accessible when making changes.



- **Network Select**
  This list is the result of a network scan. Access points with a disabled SSID Broadcast will not appear unless the camera is linked to it. The network camera is currently linked to is shown in blue. A network using unsupported security is shown in grey. The following information is provided:

  - **SSID:** The name of a wireless network (or ad-hoc device). If the same name occurs several times this means that several access points for that network were found. The camera cannot be configured to only associate with one particular access point.
  - **Security:** Shows which type of security the network uses. See below for the security types supported by the camera.
  - **Signal Level:** Shows the signal strength.

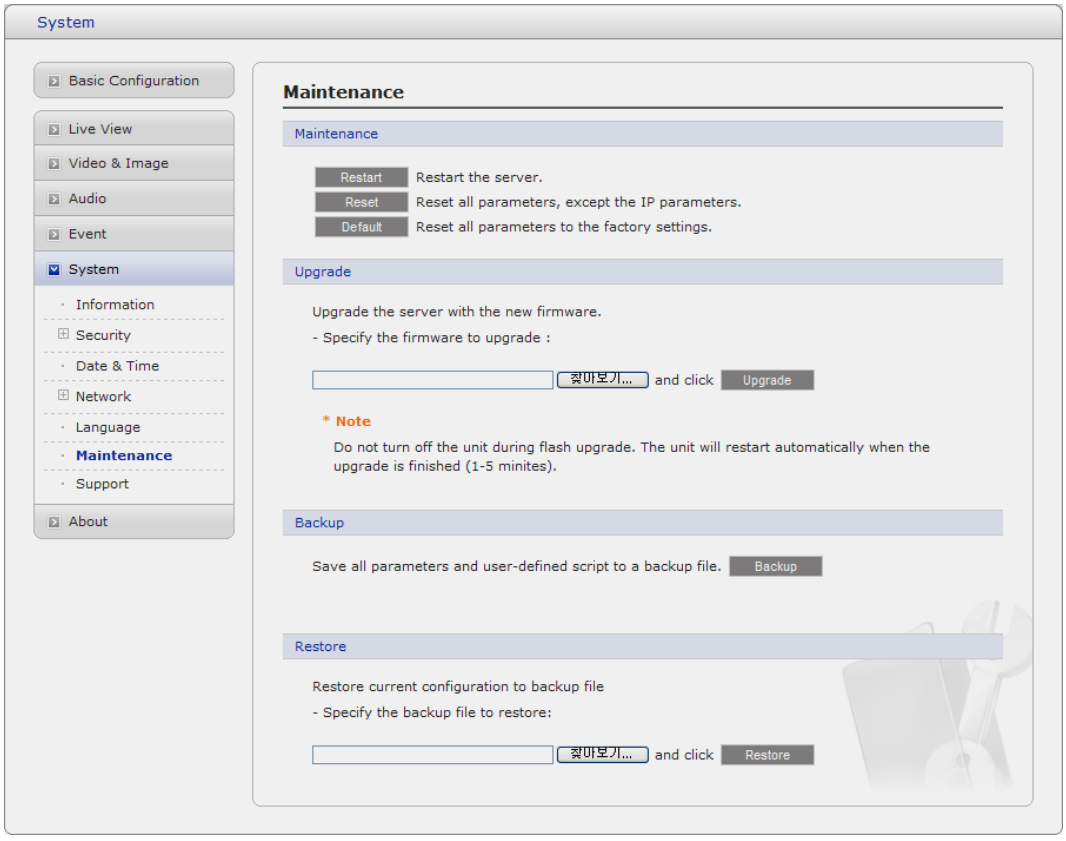
The VK2-2MPCCW has three security options:
• WPA-/WPA2-PSK
• WPA-/WPA2-Enterprise
• WEP

WPA-/WPA2-Enterprise is more secure than WPA-/WPA2-PSK, which in turn is more secure than WEP.

5) Language

It will be able to select a user language. The type of language it will be able to select is the English, the French, the German, the Spanish and the Italian.

6) Maintenance



- **Maintenance Server**
  - **Restart:** The unit is restarted without changing any of the settings. Use this method if the unit is not behaving as expected.
  - **Restore:** The unit is restarted and most current settings are reset to factory default values. The settings that are not affected are:
    * the boot protocol (DHCP or static)
    * the static IP address
    * the default router
    * the subnet mask
    * the system time

- **Default:** The default button should be used with caution. Pressing this will return all of the Network Camera's settings to the factory default values (including the IP address).

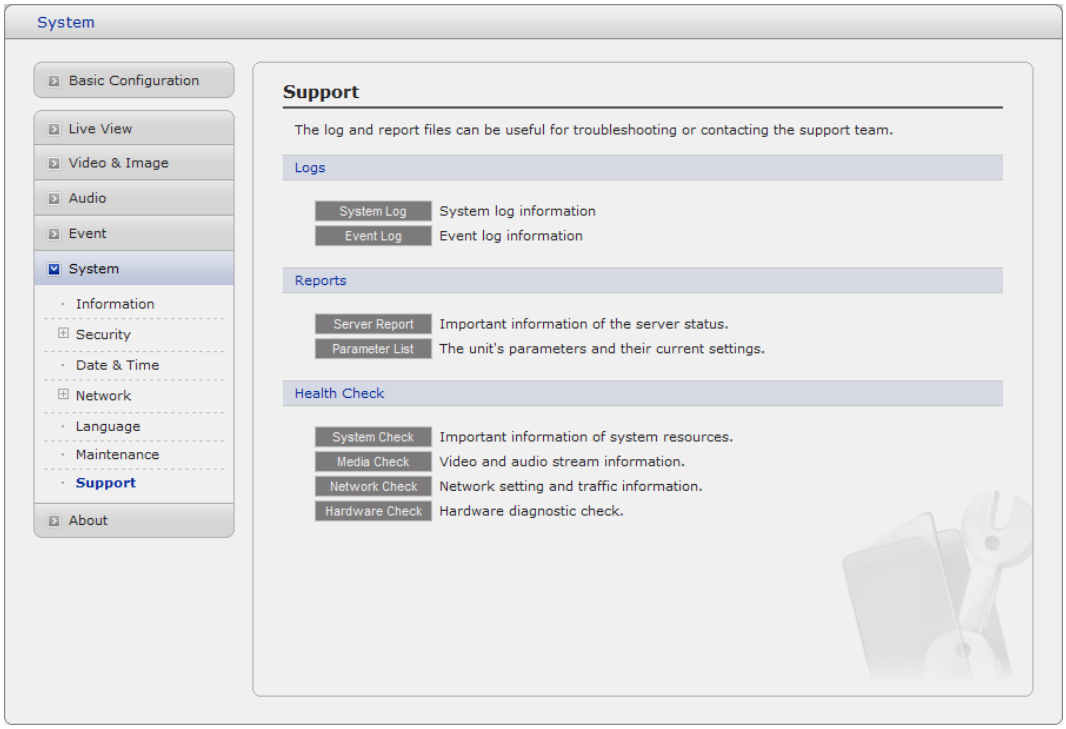
- **Update Server**
  Carry out the upgrade by importing an upgrade file and pressing the Upgrade button. During the upgrade, do not turn off the power of the Network Camera. And try an access again after waiting five minutes or longer.

- **Backup**
  Save a setting value that users enter to the Network Camera, to a user PC.

- **Restore**
  Import and apply a setting value saved to a user PC.
  Note: Backup and Restore can only be used on the same unit running the same firmware. This feature is not intended for multi-configurations or for firmware upgrades.

7) Support

The support page provides valuable information on troubleshooting and contact information, should you require technical assistance.



- **Logs**
  The network Camera support system log information. Click the System Log button to get the log data.

- **Update Server**
  - **Server Report:** Click the Server Report button to get the important information about the server's status and should always be included when requesting support.

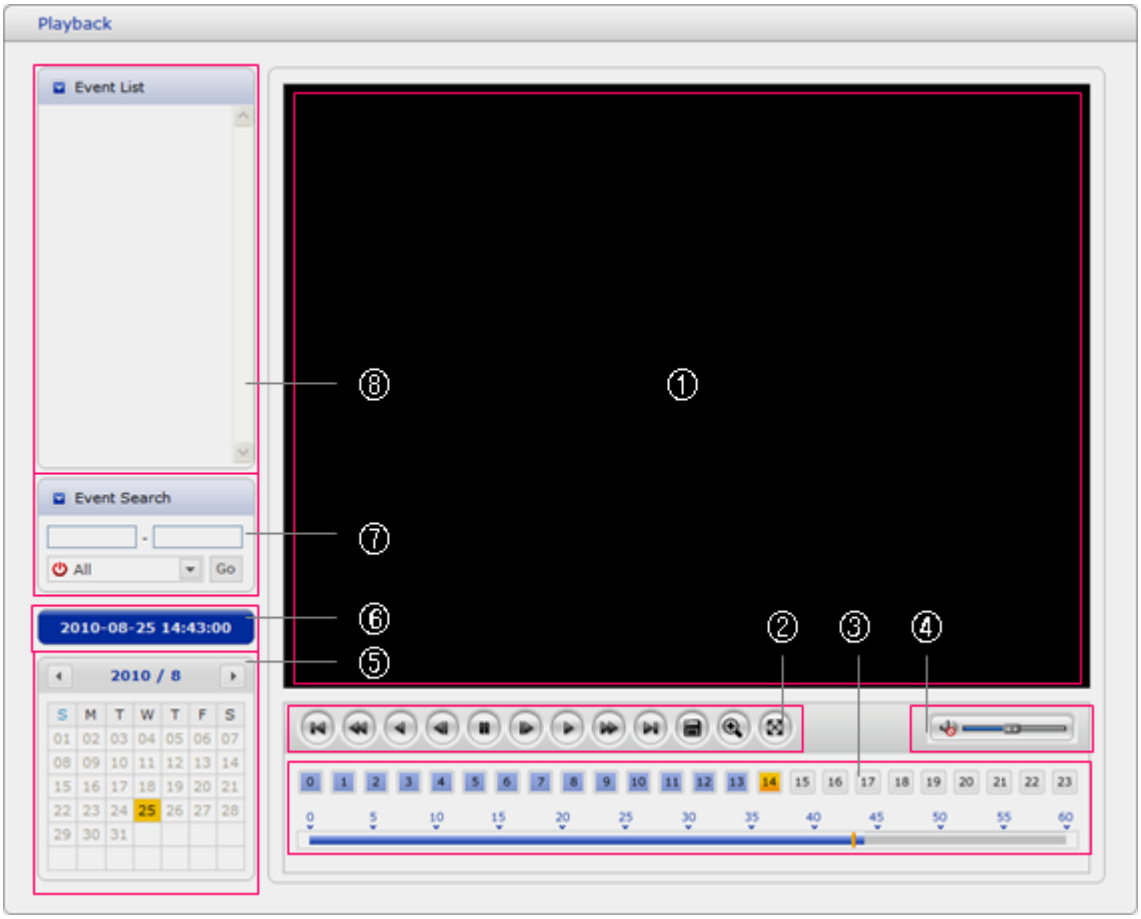
- **Parameter List:** Click the Parameter List button to see the unit's parameters and their current settings.

3.5.6 About

The following website will provide the support information for the Network Camera information and operation.

3.6 Playback

The Playback window contains a list of recordings made to the memory card. It shows each recording's start time, length, the event type used to start the recording, calendar and time slice bar indicates if the recording is existed or not.



The description of playback window follows.

(1) Video Screen
You can see the video screen when playing the video clip in the Micro SD memory

(2) Playback Buttons
To view a recording data in the SD local storage, select it from the list and click the Playback buttons.

- Go to the first: go to the beginning of the video clip.
- Fast backward play:
- Backward play: play backward of the video clip.
- Step backward play: go back one frame of the video clip.
- Pause: pause playback of the video clip.
- Step forward play: go forward one frame of the video clip.
- Forward Play: play forward the video clip.
- Fast forward play: play fast forward of the video clip.
- Step forward play: go forward one frame of the video clip.
- Clip copy: copy the video clip.
- Zoom In: zoom in the video clip
- Full Screen: display full screen of the video.

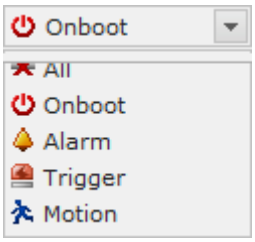
(3) Time Chart
Display an hour-based search screen for the chosen date. If there is recording data, a blue section will be displayed on a 24-hour basis. If you select a particular hour in the chart, a yellow square on the hour will be displayed.

(4) Speaker Control Bar
Use this scale to control the volume of the speakers.

(5) Search Calendar
Search results from the SD local storage in the network camera connected are displayed monthly. If there is a recorded data for a particular date, a blue square on the date will be displayed. If you select a particular date in the calendar, a yellow square on the date will be displayed.

(6) Play Time
Displays time of the video playing.

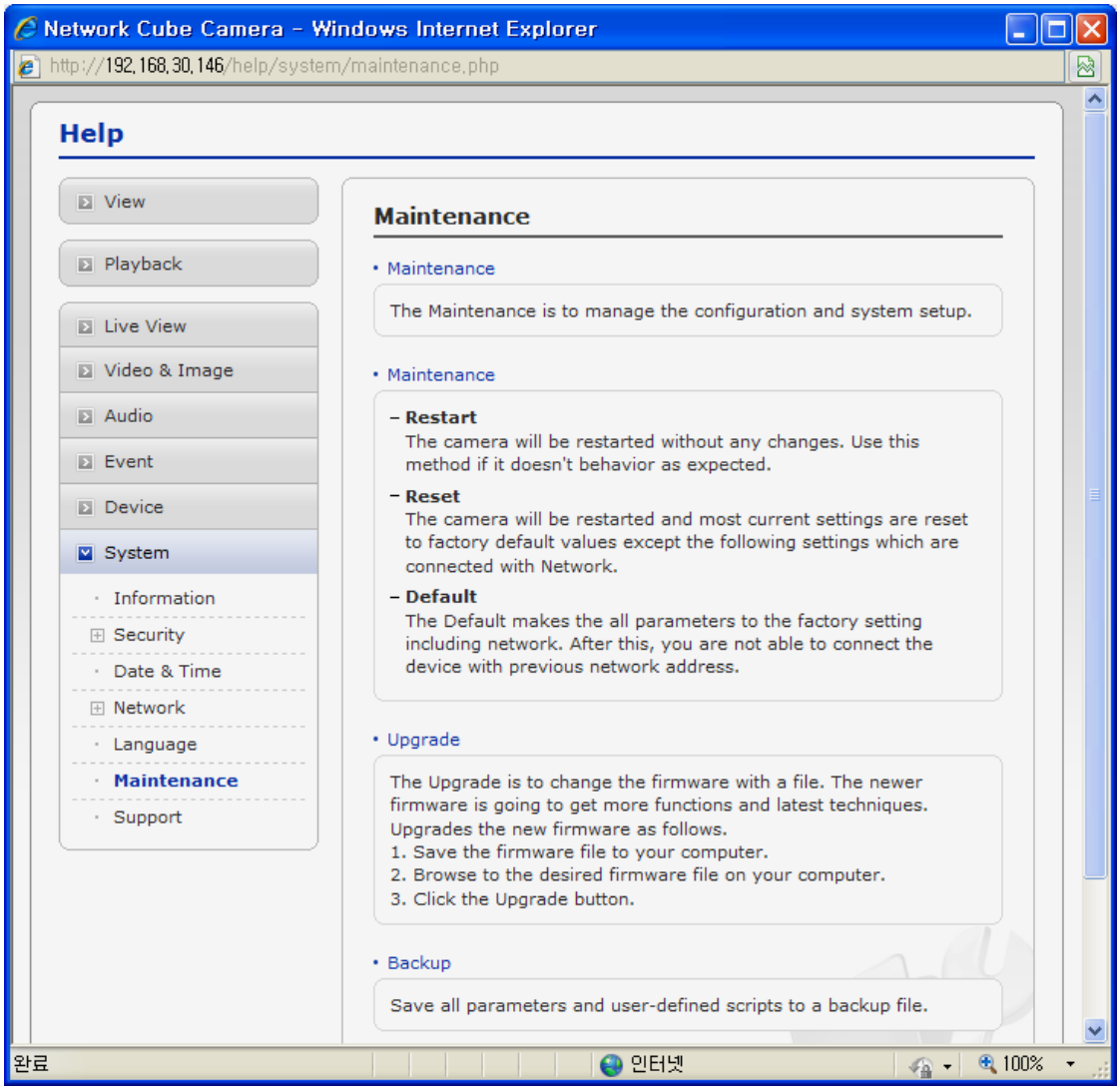
(7) Event Search Window
Select a search option in the drop-down list and click GO button. You can also enter the time period for searching. If you click Start Date or End Date zone, displays Search Calendar.



(8) Event List Window
Event List displays the event(s) that were recorded in the SD local storage. Select a list and click the play button. The video clip will be played.

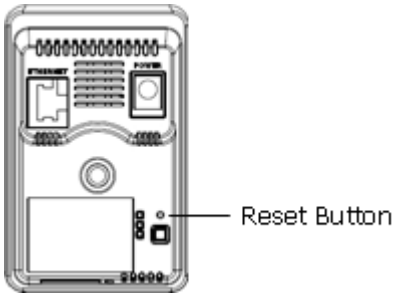
3.7 Help

The Help information window will be provided as a popup window so that users can open and read it without a need for log-in. It will offer a description on setting and Help page by which users can manipulate the Network Camera without a reference to the manual.



3.8 Resetting to the factory default settings

To reset the Network Camera to the original factory settings, go to the Setup>System> Maintenance web page (described in “3.5.4 System > Maintenance”) or use the Reset button on the network camera, as described below:



- **Using the Reset Button**
  Follow the instructions below to reset the Network Camera to the factory default settings using the Reset button.

  1. Switch off the Network Camera by disconnecting the power adapter.
  2. Press and hold the Reset button with a straightened paperclip while reconnecting the power.
  3. Keep the Reset button pressed during about 2 seconds.
  4. Release the Reset button, and wait for the Status LED to turn off.
  5. The network camera resets to factory defaults and restarts after completing the factory reset.

Caution: When performing a Factory Reset, you will lose any settings you have saved.
(Default IP 192.168.30.220)

4. APPENDIX

4.1 Troubleshooting

Troubleshooting if problems occur, verify the installation of the Network Camera with the instructions in this manual and with other operating equipment. Isolate the problem to the specific piece of equipment in the system and refer to the equipment manual for further information.

Problems/Symptoms	Possible Causes or Corrective Actions
The camera cannot be accessed by some clients.	If using a proxy server, try disabling the proxy setting in your browser. Check all cabling and connectors.
The camera works locally, but not externally.	Check if there are firewall settings that need to be adjusted. Check if there are router settings that need to be configured.
Poor or intermittent network connection.	If using a network switch, check that the port on that device uses the same setting for the network connection type (speed/duplex).
The camera cannot be accessed via a host name.	Check that the host name and DNS server settings are correct.
Not possible to log in.	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used. When attempting to log in, you may need to manually type in http or https in the browser's address bar.
No image using Refresh and/or slow updating of images.	If images are very complex, try limiting the number of clients accessing the camera.
Images only shown in black & white.	Check the Video & Image setting.
Blurred images.	Refocus the camera.
Poor image quality.	Increased lighting can often improve image quality. Check that there is sufficient lighting at the monitored location. Check all image and lighting settings.
Rolling dark bands or flickering in image.	Try adjusting the Exposure Control setting under AE and AWB part.
H.264 not displayed in the client.	Check that the correct network interface is selected in the Video & Image/Stream.
Multicast H.264 not displayed in the client.	Check with your network administrator that the multicast addresses used by the camera are valid for your network. Check that the Enable multicast checkbox are enabled in the System/Network/RTP tab. Checks with your network administrator to see if there is a firewall preventing viewing.
Multicast H.264 only accessible by local clients.	Check if your router supports multicasting, or if the router settings between the client and the server need to be configured. The TTL value may need to be increased.
Color saturation is different in H.264 and Motion JPEG.	Modify the settings for your graphics adapter. Please see the adapter's documentation for more information.
Video cannot be recorded.	Check that the SD Card is inserted properly. Check that the SD Card is formatted properly.

4.2 Product Specification

Main Item		Specification
CAMERA	Image sensor	1/4” Progressive scan RGB CMOS
	Active Array	1600(H) x 1200(V)
	Lens	Fixed 2.6mm Lens, F1.8
	Angle of View	80.7°(H) x 58.7(V) x 103.2°(D)
	Min. illumination	Color: 1Lux(LED Off), 0Lux (LED On)
	Shutter Speed	1/20,000 ~ 1/30 (Slow shutter 1/15, 1/8 and 1/4)
NETWORK	Video Compression	-. Motion JPEG -. MPEG-4 Part2 -. H.264 (MPEG-4 Part 10) -. Profiles: H.264 HP, MP, and BP, MPEG-4 SP
	Video Streaming	Simultaneously H.264(or MPEG-4) and MJPEG Controllable Frame Rate and Bandwidth VBR/CBR H.264 and MPEG-4
	Video Resolutions	320x240 ~ 1600x1200
	Frame Rate	30fps @ 1280x720, 15fps @ 1600x1200
	Audio	VK2-2MPCCPL: -. Compression: G.711 64kbps -. Streaming: 2way -. Interface: Built-in Microphone & Speaker
	Protocol	TCP/IP, UDP, IPv4/v6, HTTP, HTTPS, QoS, FTP, UPnP, RTP, RTSP, RTCP, DHCP, ARP, Zeroconf, Bonjour, Hole Punching
	Security	Multi-user authority, HTTPS, IP Filtering, Privacy Zone Wireless: WEP, WPA-PSK, WPA2 WPS: Wi-Fi Protected Setup
	Max. Connection	10
	API Programming Interface	API Supported, ONVIF(Open Network Video Interface Forum) Compliant
	Alarm Triggers	Motion Detection, Manual Trigger, Built-in PIR Sensor Audio Level Detection
	Alarm Events	-. File upload via FTP and HTTP -. Notification via E-mail, HTTP and TCP -. Built-in LED activation Audio alert activation
	Video Buffering	Pre and Post Alarm
	Motion Detection	Yes, max. 8 programmable zone
	Network Time Synchronization	Yes
	SD Recording	Yes, Event
	Software Reset	Yes
	Factory Reset	Yes, Button/Web browser
	Auto Recovery	Yes
	Installation Tool	SmartManager, VK2-Client
	Upgrade	Web browser, SmartManager, VK2-Client

GENERAL	Ethernet	RJ-45 10BASE-T/100BASE-TX VK2-2MPCCW only: Built-in IEEE 802.11b/g/n wireless LAN
	PIR Sensor	VK2-2MPCCPL only: Passive infrared (PIR) motion sensor with configurable sensitivity. Max range: 5m, 60°(H) x 20°(V)
	Illumination LED	VK2-2MPCCPL only: White illumination LED: 1 W
	Operating Temperature	0°C ~ 40°C
	Operation Humidity	0~80% (non-condensing)
	Power Consumption	DC5V 700mA / PoE 48V 73mA / 3.5W Power over Ethernet IEEE 802.3af Class0
	Dimensions (W x H x D)	62mm x 97mm x 38.4mm (without Stand)
	Unit Weight	75g

4.3 Preventive Maintenance

Preventive maintenance allows detection and correction of minor that faults before they become serious and cause equipment failure.

Every three-month, perform the following maintenance.

1. **Inspect all connection cables for deterioration or other damage.**
2. **Clean components with a clean damp cloth.**
3. **Verify that all the mounting hardware is secure.**

System Requirement for Web Browser

Operating System: Microsoft Windows 98, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows XP, or Microsoft Windows Vista
CPU: Intel Core 2 Duo 2Ghz or higher, 1GB RAM or more, 10GB free disk or higher
VGA: AGP, Video RAM 32MB or higher (1024x768, 24bpp or higher)

Norbain SD Ltd
210 Wharfedale Road
Winnersh Triangle
Wokingham
Berkshire
RG41 5TP
01189 125 302